Intentional Weakening of Encryption: The Ethical Implications of Apple's Refusal to Create a "Backdoor"

Daniel Wong

Computer Science

May 2, 2018

CPE 300

Abstract

In December of 2015, two attackers killed 14 people in San Bernardino, California. The attackers destroyed their personal phones but their work iPhones were recovered by the FBI. However, the iPhone required a 4 digit pin to unlock it. The FBI requested data from Apple through valid subpoenas and search warrants. Then, the FBI requested Apple to engineer a version of the iPhone's operating system that would allow it to disable security features once installed. Apple declined this request stating that in the wrong hands, this software can have the potential to unlock any iPhone in someone's physical possesion. Was it ethical for Apple to refuse the FBI's request to create a "backdoor" to all iPhones? [**?**]

The United States goverment urged Apple to comply with the order after being opposed. The FBI stated they would allow Apple to destroy the software once the FBI was able to unlock and remove security features of the attacker's iPhone. Critics argued that Apple and technology companies alike should be held to the same provisions which made cellular encryption weak enough to allow officials to "tap" phone conversations as seen with A5/1. Others argue in defense of Apple stating that the intentional weakening of encrpytion will lead to easy access of the encrypted data. After A5/1 was used to encrypt phone conversations, security researchers were able to attack and easily decrpyt the conversations.

Contents

1 FACTS

In December 2015, Syed Rizwan Farook and another attacker killed 14 people and seriously injured 22 others. After the attackers died, the FBI was able to recover Farook's work phone. The FBI had the National Security Agency attempt to unlock the phone. However, after a limited amount of incorrect attempts, the phone would automatically delete all of its data. With the NSA's absence of knowledge required to unlock the phone, the FBI turned to Apple and issued valid warrants and subpoenas. Apple complied and gave all of the data and information available to them.[**?**]

The FBI needs Apple's help beecause the security settings on the iPhone lock may erase all of the phone's data if passwords are entered incorrectly too many times. The FBI requested Apple to engineer an operating system that could be installed onto the attacker's phone to disable critical safety features. This operating system would allow the FBI as many trials to break the 4 digit pin without compromising the phone's encrypted data. [**?**]

Apple refused the FBI's orders to create an operating system that would circumvent several important security features and to install the operating system on the iPhone recovered during the investigation of the San Bernardino case. Apple believes that building this operating system would create a backdoor and while the government may argue that its use would be limited to this case, there is no way to guarantee such control. [**?**]

In Apple's letter to their customers, they explain that the "'key' to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge." [**?**]

Apple and other technology companies alike believe that if Apple complied and created this "backdoor", it could set a very dangerous precedent.

2 QUESTION

Was it ethically justifiable for Apple to refuse the FBI's request to create an operating system that would allow the FBI to unlock the attacker's iPhone?

3 SOCIAL IMPLICATIONS

Whether or not Apple's refusal to create a "backdoor" to unlock the phone of the San Bernardino shooter was ethical, there are numerous important considerations on its impact to the information able to be retrieved on personal phones.

When considering the implications of Apple's refusal, there are many concerns about public safety and preventing terrorism. Manhattan district attorney, Cyrus Vance, Jr., says he has 175 iPhones, with potential evidence from serious crimes, including murder, that he wants Apple to aid in opening.[26] Former FBI director, James Comey puts it, "Technology has become a tool of choice for some very dangerous people. Unfortunately, the law has not kept pace with technology and this disconnect has created significant public safety problems we have long described as 'going dark.'"[**?**] Thus, many people consider Apple's refusal to create this "backdoor" to be unjustifiable as it allows dangerous people to protect the information stored on their phone. As Republican Senator Lindsey Graham puts it during the GOP Debate in 2016, "Any system that would allow a terrorist to communicate with somebody inside our country and we can't find out what they're saying, is stupid."[**?**]

On the contrary, many argue that if this "backdoor" was built, it could lead to huge privacy concerns for the general public. John Oliver explains, "If you penetrate a safe, you have only penetrated that safe. But, a code to open one phone could be modified to work on many more phones."[**?**] Apple's CEO Tim Cook comments, "No one, I believe, would want a master-key built

that would turn hundreds of millions of locks even if that key were in the possesion of the person that you trust the most; that key can be stolen... The only way we know to get additional information is to write a piece of software that is the software equivalent of cancer."[?] Thus, this order and compliance has many important implications regarding overall security of the public including their privacy and preventing terrorism.

4 EXTERNAL ARGUMENTS

4.1 Encryption: Last Week Tonight with John Oliver (HBO)

In an influential piece by John Oliver, he argues that whatever happens in this case will have huge rammifications. "Because, the FBI ultimately wants Apple and the entire technology industry to have an encryption always be weak enough that the company can access customer's data if law enforcement needs it." [?].

4.2 Matt Blaze: A key under the doormat isn't safe. Neither is an encryption backdoor.

Matt Blaze, an associate professor in the Computer Science Department at the University of Pennsylvania, "studies secure systems cryptography and the impact of technology on public policy." In 1993, the "Clipper Chip" was invented by the NSA and was as a device that would encrypt consumer computer's data but allow officials to access the data if needed. However, Matt Blaze was able to exploit the security flaws in the system. "Clipper's failure starkly demonstrated that cryptographic backdoors must be understood first as a technical problem... Clipper failed not because the NSA was incompetent, but because desigining a system with a backdoor was - and still is - fundamentally in conflict with basic security principles." [?]

4.3 Manhattan District Attorney: Smartphone Encryption and Public Safety

The Manhattan District Attorney's office believes that Apple and technology companies alike are making encryption decisions based on their business interests rather than considering the public's safety interests. "Without legislative action, these corporations will 'continue' to focus on customer and shareholder value,' while government entities 'will try to demonstrate the critical public safety price they (meaning we) pay for 'warrant-proof' platforms'." [26]

5 HOW THE SOFTWARE ENGINEERING CODE OF ETHICS APPLIES

The IEEE/ACM Softwar Engineering Code of Ethics considers software engineers to be those who "contribute by direct participation ... to the analysis, specification, design, development, ... and testing of software systems." [?] The operating system is the essential piece of software which interfaces between the user and hardware. "An operating system is a software which performs all the basic tasks like file management, (and) memory management" [?]

Thus, the employees at Apple whom are tasked with creating and maintaining critical safety features on the operating system are considered Software Engineers. These employees "shall adhere to the [Software Engineering] Code of Ethics and Professional Practice" [?] Software Engineers at Apple are the ones responsible for creating the operating system that fully encrypts and protects the data stored on iPhones from becoming breached. The IEE/ACM Software Engineering Code of Ethics states that "Because of

their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm." [**?**] Is Apple instructing their software engineers to do good or cause harm?

6 ANALYSIS

6.1 Tenet 1.04: Potential Danger

Tenet 1.04 of the SE Code of Ethics requires software engineers to "disclose to appropriate persons ... any actual or potential danger to the user ... that they reasonably believe to be associated with software or related documents" [23].

6.1.1 Definitions

6.1.1.1 Disclosure to Appropriate Persons

To "disclose" is to "make known, reveal, or uncover" [8]. In the context of research, disclosure is closely related to informed consent, which the Institutional Review Board Guidebook claims "assures that prospective human subjects will understand the nature of the research and can knowledgeably and voluntarily decide whether or not to participate" [19]. This definition regards prospective human subjects as the appropriate persons to which disclosure is directed. According to these definitions, to "disclose to appropriate persons" in research means to "make known to prospective human subjects (users)", and disclosure should include an opportunity to decide whether or not to participate in the research.

6.1.1.2 Actual or Potential Danger

"Danger" is defined as "liability or exposure to harm or injury; risk; peril" [6]. According to the Research Ethics Guidebook, "harm in social science research includes quite subjective evaluations like distress, embarrassment, and anxiety" [18]. This definition is relevant because social science is "the study of society and social behavior" [15], and Facebook's "emotional contagion" study "tested whether exposure to emotions led people to change their own posting behaviors" [**?**]. Therefore, "actual or potential danger" may be defined as "potential risk of distress, embarrassment, or anxiety".

6.1.1.3 Reasonable Belief

Reasonable belief may be defined as "hav[ing] knowledge of facts which, although not amounting to direct knowledge, would cause a reasonable person, knowing the same facts, to reasonably conclude the same thing" [20]. In other words, reasonable belief requires evidence, but not necessarily proof. To "reasonably believe", then, means to "have evidence to believe".

6.1.2 Domain Specific Rule

In the domain of internet research, tenet 1.04 requires Facebook's software engineers to "make known to users ... any potential risk of distress, embarrassment, or anxiety to the user ... that they have evidence to believe is associated with the Facebook news feed algorithm."

6.1.3 Discussion

6.1.3.1 Potential Risks

One major defense of Facebook is Tal Yarkoni's "In Defense of Facebook" article, which questions whether the "emotional contagion" experiment was any different from routine updates to Facebook. Yarkoni argues that "every single change Facebook makes to the site alters the user experience", and that these updates are made in the interest of improving the user experience [32]. Michelle Meyer agrees, arguing that the "emotional contagion" experiment was ultimately designed to improve the user experience, and that it did not "mess with people's minds" any more than Facebook usually does [28].

It is important to note, however, that the "emotional contagion" experiment was not con-

ducted as a routine update to the system; it was designed to test "whether emotional contagion occurs outside of in-person interaction between individuals" [**?**]. Adam Kramer, one of the study's authors, stated that the researchers' "goal was never to upset anyone" [29]. The intentions of the study, however, are irrelevant to the potential for harm, which may have been necessary for the experiment to yield beneficial results. Kramer goes on to acknowledge that the study resulted in harm to the subjects: "the research benefits of the paper may not have justified all of [the] *anxiety*" [emphasis added]. Did the researchers have evidence to believe that the changes made for the experiment might cause anxiety before the study was conducted?

The paper on the study makes references to previous studies on "emotional contagion": "Emotional contagion is well established in laboratory experiments, with people transferring positive and *negative emotions* to others. Data from a large real-world social network, collected over a 20-y period suggests that longer-lasting moods (e.g., *depression*, happiness) can be transferred through networks" [emphasis added] [**?**]. These references are clear acknowledgments that the phenomenon of "emotional contagion" has been demonstrated to include the spreading of negative emotions (including the anxiety that Kramer acknowledged). As the study was designed to examine "emotional contagion" via Facebook News Feeds, the researchers must have considered the possibility that negative emotions could be successfully spread during the experiment. Therefore, the studies cited in the paper constitute sufficient evidence for the potential risk of negative emotions, including anxiety, associated with the software relevant to the experiment.

6.1.3.2 Making Risks Known

If the researchers had sufficient evidence for potential risk, did they make these risks known to the subjects of the experiment?

As previously mentioned, disclosure is an important component of informed consent [19]. The researchers state that because they did not personally see any user data, the experiment "was consistent with Facebooks Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent" [**?**]. James Grimmelmann agrees that this is "a meaningful way of avoiding privacy harms", which is a "principle risk" in observational studies [24]. However, he goes on to point out that the "emotional contagion" study was an experimental study, which carries more potential risks than just privacy risks. Indeed, the paper does not directly address other potential risks associated with informed consent, including the risk of distress, embarrassment, or anxiety.

If the researchers claim that Facebook's Data Use Policy constitutes informed consent, does it also address these risks? The policy states that Facebook "may use the information [it] receive about [users]: ... for internal operations, including troubleshooting, data analysis, testing, *research* and service improvement" [emphasis added] [27]. However, Kashmir Hill points out that the term "research" was added four months after the study was conducted [25]. This means that the Data Use Policy could not have been considered notification of participation in the study at the time it was conducted. As many critics point out, Facebook did not provide any explicit notification of participation in the study, and it was conducted without the subjects' knowledge [29] [25] [27] [31]. Therefore, the subjects could not have been aware of any potential risks associated with the experiment, since they were not even aware that they were subjects of an experiment in the first place.

6.1.4 Conclusion

The researchers behind Facebook's "emotional contagion" study had evidence to believe in potential risks of anxiety to human subjects associated with the software used in the experiment. The domain specific rule above, derived from tenet 1.04 of the Software Engineering Code of Ethics, states that they were required to make

these risks known to the participants of the experiment. Because participation in the study was not made known to the subjects, they could not have been aware of these potential risks, and this rule was not satisfied.

6.2 Tenet 2.03: Knowledge and Consent

Tenet 2.03 of the SE Code of Ethics requires software engineers to "use the property of a client ... only in ways properly authorized, and with the client's ... knowledge and consent" [23].

6.2.1 Definitions

6.2.1.1 Property

Digital content consists of "individual files such as images, photos, videos, and text files ... stored either on a device owned by an individual (locally), or on devices accessed via the Internet (in the cloud), often as part of a service offered by a third party and governed by a contact with the individual", and digital content can be considered "intangible, personal property" [30]. User generated content is defined as "published information that an unpaid contributor has provided to a web site", which can include "a photo, video, blog or discussion forum post, poll response or comment made through a social media web site" [22]. Because social media posts are user generated content, a form of digital content, and digital content is considered personal property, social media posts can be considered property. In the context of social media, "property" therefore includes "social media posts".

6.2.1.2 Client

A client is "a customer or a person who uses services" [3]. A service "[supplies] public communication" [13]. Social media is defined as a form "of electronic communication... through which users create online communities to share information" [14]. Because social media supplies public communication, it can be considered a service. Therefore, "clients" includes "users" of social media software.

6.2.1.3 Proper Authorization, Knowledge, and Consent

To authorize is to "give official permission for or approval to" [2], and consent is "permission for something to happen" [5]. Because authorization and consent are explicit actions, they cannot be properly given without adequate knowledge of the situation, and knowledge can be considered a necessary component of consent and authorization. Given the overlap between consent and authorization, and the necessity of knowledge in both, "proper authorization, knowledge, and consent" can be simplified to "official approval".

6.2.2 Domain Specific Rule

In the domain of social media, tenet 2.03 requires software engineers to "use the social media posts of a user only in ways officially approved by the user."

6.2.3 Discussion

As previously mentioned, Facebook researchers claimed that the "emotional contagion" study was conducted in accordance with Facebook's Data Use Policy, which they cite as sufficient informed consent [**?**]. In order to justify this claim, the use of user posts in the experiment must be compared with the Data Use Policy, both of which will be examined in the following sections.

6.2.3.1 Use of Users' Posts

In what ways did the Facebook researchers use the users' posts?

The "emotional contagion" paper states that user posts were analyzed by the "Linguistic Inquiry and Word Count software (LIWC2007) word counting system" in order to determine whether they were positive or negative [**?**]. This

data was then used to determine the posts' likelihood of omission from the users' news feeds according to the experimental condition they were assigned to. No new posts were added to the users' news feeds; the experiment only involved post omission. Finally, the paper makes clear that all posts were still accessible via the poster's personal "timeline", and that no personal private messages were affected by the experiment [**?**].

To summarize, user posts were analyzed for emotional content and used in the experiment to skew the prevalence of positive or negative posts in participants' news feeds.

6.2.3.2 What The Data Use Policy Authorized

What did Facebook users approve of by agreeing to Facebook's Data Use Policy?

In May 2012, Facebook amended its Data Use Policy, adding a line stating that user data may be used "for internal operations, including troubleshooting, data analysis, testing, *research* and service improvement" [25]. Prior to this amendment, which was made *four months* after the "emotional contagion" experiment was conducted, there was no mention of research in the document.

A number of critics of the experiment refer to the updated Data Use Policy without stating that this line did not appear in the document when the experiment was conducted [25]. Thomas Leeper, in his analysis on the ethics of the experiment, argues that agreeing to the policy gives Facebook permission to use user data as long as it is "de-identified", a statement he justifies with the following line from the policy: "we don't share information we receive about you with others unless we have: received your permission; given you notice, such as by telling you about it in this policy; *or* removed your name and any other personally identifying information from it" [27]. While the data was analyzed in an anonymous fashion, Leeper's defense leaps to authorizing Facebook to "use [user] data however [it] want[s]" even though this line only authorizes sharing of anonymous data. While the previously mentioned line regarding research may have provided such authorization, the latter does not address usage outside of sharing anonymous data, and therefore does not constitute official approval of the experiment by users.

6.2.4 Other Means of Authorization

If the Data Use Policy did not provide official approval at the time of the study, was there some other way Facebook gained approval for the use of user posts in the experiment?

One way to gain approval for the experiment would be to request it directly from the participants. However, as discussed in section 6.1.3.2, Facebook did not provide explicit notification of participation in the experiment. Even if participants had been notified, though, such notification would only have been relevant to participants' data. Because the experiment involved filtering posts from the participants' friends, Facebook would have needed approval from non-participants as well. Because notification of the experiment was not provided to either the participants or their friends (see Section 6.1.3.2), Facebook could not have gotten approval for the experiment from them directly.

6.2.5 Conclusion

The researchers behind Facebook's "emotional contagion" study used user data for the purposes of research and experimentation, and they cited Facebook's Data Use Policy as informed consent. Though this document may have constituted official approval for the use of user posts in the experiment, provisions for use in research were not added until four months after the experiment was conducted; no mention of research was made in the document at the time the experiment was conducted. In addition, no notification of the experiment was provided to participants or other users whose posts were used for the purposes of the experiment; the Data Use Policy was the only document through which Facebook attempted to

gain approval for the use of user posts. Because this document did not mention research or experimentation at the time of the study, it did not sufficiently gain this approval. The experiment therefore used user data in ways not officially approved by the user, and was in violation of the domain specific rule derived above from tenet 2.03 of the Software Engineering Code of Ethics.

6.3 Tenet 2.05: Privacy

Tenet 2.05 of the SE Code of Ethics requires software engineers to "keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law" [23].

6.3.1 Definitions

6.3.1.1 Keeping Private

In the context of digital data, privacy "deals with the ability an ... individual has to determine what data in a computer system can be shared with third parties" [21]. More generally, privacy is "the state or condition of being free from being observed or disturbed by other people" [10]. These definitions suggest that to "keep private" is to "maintain freedom from observation by other people".

6.3.1.2 Confidential Information

Something that is "confidential" can also be considered "secret or private" [4]. Given the above definition of privacy, "confidential information" means information of which access to third parties is determined by the owner of the information. Because data is information [7], and data is the relevant information in social media, "confidential information" means "data that is intended to be accessed only with permission of the owner". As discussed in Section 6.2.1.1, the relevant data is a user's social media posts, and the owner is the user who generated that data. Because Facebook's privacy settings provide users with the opportunity to decide who has permission to see their posts [1], "data that is intended to be accessed only with the permission of the owner" includes social media posts. Therefore, "confidential information" includes "social media posts".

6.3.1.3 Professional Work

Something that is "professional" "relat[es] to a job that requires special education, training, or skill" [11]. Because "a software engineer is a licensed professional engineer" [16], "work done in a software engineering job" can be considered "professional work". Because the Facebook researchers are software engineers (see Section 4), the "emotional contagion experiment" is the relevant professional work.

6.3.1.4 Public Interest

"Public interest", though a nebulous concept, is defined as "the welfare or well-being of the general public" [12]. Without getting into too much detail, "public interest" is "the welfare of the general public".

6.3.2 Domain Specific Rule

In the domain of social media research, tenet 2.05 requires software engineers to "maintain freedom from observation by other people any social media posts gathered during the 'emotional contagion' experiment, where such confidentiality is consistent with the welfare of the general public and consistent with the law".

6.3.3 Discussion

6.3.3.1 What Was Gathered During the Experiment?

As mentioned in Section 6.2.3.1, social media posts were gathered for the 689,003 users who were involved in the experiment. These posts include those made by the participant users, but

also users they are connected to whose posts were filtered by the news feed algorithm. This amounted to a total of roughly 3 million posts [**?**].

6.3.3.2 Who Observed the Data?

Also mentioned in Section 6.2.3.1, the "emotional contagion" paper states that posts were analyzed by the "Linguistic Inquiry and Word Count software (LIWC2007) word counting system" for the presence of positive or negative content, and that "no text was seen by the researchers" [**?**]. As mentioned in 6.1.3.2, James Grimmelmann agrees that "automated data processing is a meaningful way of avoiding privacy harms to research subjects" in spite of his criticism of the study [24]. Because the users' posts were analyzed by software and not seen by people, the researchers did "maintain freedom from observation by other people" with regards to social media posts.

6.3.3.3 Welfare of the General Public and the Law

If the researchers complied with the domain specific rule in maintaining the privacy of user data, are there any reasons why this was not consistent with the public good or the law?

Experimental psychology is defined as "the branch of psychology dealing with the study of *emotional...* activity... in humans... by means of experimental methods" [9]. Because the "emotional contagion" experiment studied emotional activity, it can be considered a psychological experiment. The American Psychological Association has a code of ethics that addresses disclosure of confidential information. The APA Ethical Standard 4.05 justifies the disclosure of confidential information when permitted or mandated by law, or for valid purposes such as protection of "the client/patient, psychologist, or others from harm" [17]. This standard also states that "the legal duty [of disclosure] is based upon a clinical assessment".

Would observation of the user data have protected anybody from harm? The users' posts were only analyzed for the purposes of finding positive or negative content, and the analysis was only used to tag posts as positive or negative for omission from the news feed. Because of this, researchers could not have been able to determine whether posts demonstrated a risk of harm to anybody. Furthermore, as the data was not assessed by the researchers, there could not have been any legal duty to disclose information.

6.3.4 Conclusion

The Facebook researchers who conducted the "emotional contagion" experiment gathered roughly 3 million social media posts for the purposes of the experiment. The domain specific rule derived above from tenet 2.05 of the Software Engineering Code of Ethics mandates protection of this data from being observed by other people unless justified by the interests of the public good or the law. Because the data was analyzed by software without being seen by people, it was successfully protected from observation. Furthermore, because the posts were not assessed, no legitimate risk of harm could have been found to justify the disclosure of the data as consistent with the welfare of the general public or the law. Therefore, the experiment was conducted in compliance with the domain specific rule, and tenet 2.05 from which it was derived.

6.4 Conclusions of Analysis

To summarize the conclusions of the prior analysis, the "emotional contagion" experiment conducted by Facebook researchers was in violation of tenets 1.04 and 2.03 of the Software Engineering Code of Ethics, but was in compliance with tenet 2.05. The researchers had sufficient evidence for potential risks of anxiety to participants, and were required to make those risks known to the participants according to tenet 1.04. Because participation in the study was

not made known to the participants, they could not have been aware of these risks. In addition, this lack of notification shows that the participants could not have given official approval for the use of their data in the experiment, as required by tenet 2.03. Though Facebook claims the Data Use Policy is sufficient for gathering this approval, the document did not mention research until four months after the study, and therefore could not have gathered official approval at the time of the experiment. Finally, because the posts were analyzed by software and were not seen by the researchers, the privacy of confidential information (users' posts) was maintained in accordance with tenet 2.05. As no assessment was made of the data, there could not have been justification for disclosure according to the welfare of the general public or the law.

References

[1] Basic privacy settings & tools. https://www.facebook.com/help/325807937506242/. Facebook privacy settings suggest that users are in control of who sees their data.

[2] Definition of authorize. http://www.oxforddictionaries.com/us/definition/american_english/authorize. Formal definition of authorize.

[3] Definition of client. http://www.yourdictionary.com/client. Formal definition of client.

[4] Definition of confidential. http://www.merriam-webster.com/dictionary/confidential. Formal definition of confidential.

[5] Definition of consent. http://www.oxforddictionaries.com/us/definition/american_english/consent. Formal definition of consent.

[6] Definition of danger. http://www.dictionary.com/browse/danger. Formal definition of danger.

[7] Definition of data. http://www.dictionary.com/browse/data. Formal definition of data.

[8] Definition of disclose. http://www.dictionary.com/browse/disclose. Formal definition of disclosure.

[9] Definition of experimental psychology. http://www.dictionary.com/browse/experimental-psychology. Formal definition of experimental psychology.

[10] Definition of privacy. http://www.oxforddictionaries.com/us/definition/american_english/privacy. Formal definition of privacy.

[11] Definition of professional. http://www.merriam-webster.com/dictionary/professional. Formal definition of professional.

[12] Definition of public interest. http://www.dictionary.com/browse/public-interest. Formal definition of public interest.

[13] Definition of service. http://www.dictionary.com/browse/service. Formal definition of service.

[14] Definition of social media. http://www.merriam-webster.com/dictionary/social%20media. Formal definition of social media.

[15] Definition of social science. http://www.dictionary.com/browse/social-science. Formal definition of social science.

[16] Definition of software engineer. http://www.webopedia.com/term/s/software_engineer.html. Formal definition of software engineer.

[17] Disclosing confidential information. http://www.apa.org/monitor/2014/04/disclosing-information.aspx. APA guidelines for the disclosure of confidential information.

[18] How is harm defined? http://www.ethicsguidebook.ac.uk/how-is-harm-defined-67. Discusses and defines harm in research.

[19] Irb guidebook chapter iii: Basic irb review. http://www.hhs.gov/ohrp/archive/irb/irb_chapter3.htm. HHS formal requirements for Information Review Board informed consent.

[20] Legal definition of reasonable cause to believe. http://www.lectlaw.com/def2/q015.htm. Legal definition of reasonable belief.

[21] What is data privacy (information privacy)? http://searchcio.techtarget.com/definition/data-privacy-information-privacy. Formal definition of information privacy.

[22] What is user-generated content (ugc)? http://searchcio.techtarget.com/definition/user-generated-content-ugc. Formal definition of user generated content.

[23] Software engineering code of ethics and professional practice. http://www.acm.org/about/se-code, 2015. Citation for the full text of the SE Code of Ethics.

[24] Grimmelmann, J. As flies to wanton boys. http://laboratorium.net/archive/2014/06/28/as_flies_to_wanton_boys, Jun 2014. Raises strong concerns about informed consent, and discusses the particular requirements provided in the Federal Policy for the Protection of Human Subjects (the "Common Rule").

[25] Hill, K. Facebook added 'research' to user agreement 4 months after emotion manipulation study. http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/ Jun 2014. Forbes article that discusses changes to Facebook's Data Use Policy four months after the "emotional contagion" study.

[26] Kramer, A. D. I., Guillory, J. E., and Hancock, J. T. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences 111*, 24 (Feb 2014), 87888790. Reference to Facebook's "emotional contagion" study.

[27] Leeper, T. J. Science, social media, and the boundaries of ethical experimentation. http://thomasleeper.com/2014/06/facebook-ethics/, Jun 2014. Defends Facebook's allegations that its Data Use Policy covers informed consent.

[28] Meyer, M. N. Misjudgements will drive social trials underground. http://www.nature.com/news/misjudgements-will-drive-social-trials-underground-1.15553, Jul 2014. Raises concerns about the effects of outrage on the publicity of big data research, and points out that this research could have been conducted quietly without the public's knowledge.

[29] Meyer, R. Everything we know about facebook's secret mood manipulation experiment. http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/, Jun 2014. Provides a comprehensive analysis of the facts surrounding the "emotional contagion" controversy.

[30] Romano, J. A working definition of digital assets. http://www.thedigitalbeyond.com/2011/09/a-working-definition-of-digital-assets/comment-page-1/, Sep 2011. Definitions of digital assets and digital property.

[31] Waldman, K. Facebooks unethical experiment manipulated users emotions. http://www.slate.com/articles/health_and_science/science/2014/06/facebook_unethical_experiment_it_made_news_feeds_happier_or_sadder_to_manipulate.html, Jun 2014. Argues that Facebook's Data Use Policy is insufficient for the provision of informed consent.

[32] Yarkoni, T. In defense of facebook. http://www.talyarkoni.org/blog/2014/06/28/in-defense-of-facebook/, Jun 2014. Stresses the importance of the insignificant effects found in the study and considers the "big picture" of data usage issues.