ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35680

# Cybersecurity Issues in Crowdsourcing Engineering Initiatives

**Dr. Donna M. Schaeffer, Marymount University**

Dr. Donna M. Schaeffer is a Professor in the School of Technology and Innovation at Marymount University.

**Ms. Jillian Drake, Marymount University**

Ms. Jillian Drake is a Doctorial Student in the School of Technology and Innovation at Marymount University.

# Cybersecurity Issues in Crowdsourcing Engineering Initiatives

## Abstract

As crowdsourced and open innovation engineering-related projects become more wide-spread and globally orientated, we must pay attention to cybersecurity issues that can emerge. The sharing of data and personally identifiable information are fundamental aspects of crowdsourcing and open innovation initiatives, necessitating the evaluation of the cybersecurity concerns of user privacy, data confidentiality, data integrity and system availability. Lapses within any area of the cybersecurity realm can result in damages to reputation, cause for legal damage or regulatory action.

Governance of crowdsourced projects must include attention to both ethical considerations, as well as cybersecurity issues, regardless of their scope and scale. The exploitation of cybersecurity vulnerabilities are often result from ethical omissions or oversights. Just as engineers respect engineering professional ethics, so must citizens who participate in crowdsourcing or open innovation endeavors which solicit, gather or process data.

Taxonomies provide a useful mechanism to understand and classify various social or technical phenomenon. In this paper, we will share a taxonomy that identifies how professional engineering ethics are represented and brought to life in 21st century crowdsourced engineering projects, which include commercial and research efforts from Dell Technologies, Ennomotive, Innocentive, IDEO, Digital Humanitarian Network, the Humanitarian OpenStreetMap Team, and the United States' government Challenge.gov initiative.

**Keywords:**
**Crowdsourcing, Open Innovation, Engineering Ethics, Taxonomy**

## 1.0 Introduction

As crowdsourced and open innovation engineering-related projects become more wide-spread and globally orientated, we must pay attention to cybersecurity issues that can emerge. The sharing of data and personally identifiable information are fundamental aspects of crowdsourcing and open innovation initiatives, necessitating the evaluation of the cybersecurity concerns of user privacy, data confidentiality, data integrity and system availability. Lapses within any area of the cybersecurity realm can result in damages to reputation, cause for legal damage or regulatory action.

Governance of crowdsourced projects must include attention to both ethical considerations, as well as cybersecurity issues, regardless of their scope and scale. The exploitation of cybersecurity vulnerabilities are often result from ethical omissions or oversights. Just as engineers respect engineering professional ethics, so must citizens who participate in crowdsourcing or open innovation endeavors which solicit, gather or process data.

## 1.1 Crowdsourcing

"Crowdsourcing", a term first coined by Wired Magazine editors Howe and Robinson in 2005, conceptualizes the concept of outsourcing a task or project from an internal source to a large network of people who are engaged through an open call [12]. One of the first recorded examples of crowdsourcing was when in 1714 the British Government offered €20,000 to whomever could discover a solution to finding longitude while at sea. The contest was eventually solved by, and the money awarded to John Harrison who invented the Marine Chronometer as a solution [5]. Though taking place over 300 years prior, similar crowdsourcing practices are alive and well today. Currently, crowdsourcing, also known as open innovation, takes place across industries in the form of competitions, collaboration and knowledge gathering.

Crowdsourcing and open innovation are currently looked at as a source for "creative and beneficial solutions" to a variety of problems and will likely become more prevalent in the future [3]. Crowdsourcing is already proving promising in providing new technology within industry sectors including health, manufacturing, automotive, smart infrastructure, as well as many others [2]. In engineering specifically, crowdsourcing and open innovation initiatives can be used to engage students, create life-saving solutions to problems and connect people across countries. Many companies such as Ennomotive [9] and InnoCentive [15] encourage and fund crowdsourced engineering initiatives in which anyone can take part.

As crowdsourced and open innovation engineering-related projects have become more wide-spread and global, cybersecurity and ethical issues can emerge[35]. Cybersecurity and ethical issues can arise at any phase within the crowdsourcing project, from recruitment and project initiation, through the work phase, as well as to the completion and acceptances phases. It is essential that vulnerabilities for each phase of the crowdsourcing project be identified and addressed [29]. Crowdsourcing and open innovation initiatives rely heavily upon a volunteer and free-lance workforce and as such, often common privacy and confidentiality safeguards could be overlooked due to a perceived lack of regulatory oversight required. [18]. While many crowdsourced and open innovation initiatives ethically promote humanitarian goals, some projects focus on recruiting participants to provide false input data to adversely affect machine learning, artificial intelligence systems or consumer behavior [25].

## 1.2 Engineering Professional Ethics

Codes of ethics set the standards for professional behavior within a given society. A standard of behavior then allows for a foundation of trust that ensures the public's best interest is always paramount. Within engineering this is critical since the work of engineers can affect public health and safety, business practices, and politics [3]. The National Society of

Professional Engineers (NSPE) relies on the "Code of Ethics for Engineers" which states Engineers, in the fulfillment of their professional duties, shall:

1. Hold paramount the safety, health, and welfare of the public.
2. Perform services only in areas of their competence.
3. Issue public statements only in an objective and truthful manner.
4. Act for each employer or client as faithful agents or trustees.
5. Avoid deceptive acts.
6. Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession. [22].

Additionally, the NSPE provides several engineering professional obligations which reflect their stated ethics which include the requirement that "Engineers shall be guided in all their relations by the highest standards of honesty and integrity." This overarching declaration covers many of the other NSPE's engineering obligations regarding acting ethically in regard to the acceptance, financial compensation, and appropriate attribution of credit for work done, as well as professional conduct. However, while following standards of practice can serve as a guideline to ethical behavior but it is not a catchall. Though the NSPE code of ethics seems thorough, NSPE strictly states that "A code of ethics is not a static document, its purpose is to live and breathe with the Profession it serves" [22].

Within the cybersecurity realm, the International Information Systems Security Certification Consortium (ISC)$^2$ organization states, "The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior." [6]. Believing ethical behavior is a core foundational principle for practicing cyber professional, the (ISC)$^2$ organization provides an additional set of cannons which include one's responsibility to:

1. Protect society, the common good, necessary public trust and confidence, and the infrastructure.
2. Act honorably, honestly, justly, responsibly, and legally.
3. Provide diligent and competent service to principals.
4. Advance and protect the profession. [6].

In contrast, unethical behavior is described as the unwillingness to adhere to proper rules of conduct [20]. Typically, unethical decisions are based on convenience, the desire to win or seek profit, or a rationalization of choices using relativism [19]. Organizational engineering processes or initiatives within any organization can be negatively impacted through unethical behaviors such as financial misconduct, corruption, bribery, design or material shortcuts, and any type of deceit [10]. Unethical behavior can result in health and safety issues, client income loss or cost overruns, as well as potential negative impacts on the engineering industry reputation [33].

### 1.3 Cybersecurity Challenges in Crowdsourced Engineering Initiatives

Although, crowdsourcing is increasingly being adopted as a practice for open innovation, there are challenges regarding the identification of risks associated with the adoption of a crowdsourcing model [35]. The CIA cybersecurity triad which represents the concepts of information confidentiality, integrity and availability is a valuable reference for the evaluation of security risks and be applied within this context [29]. Information confidentiality is maintained through the prevention of unauthorized disclosure of information and is frequently ensured through controls related to network access, authentication, and encryption methodologies [21]. Closely related to confidentiality is the concept of privacy which at the highest level is defined by NIST as “The right of a party to maintain control over and confidentiality of information about itself.” [23]. The concept of data integrity is concerned with the unauthorized alteration of information, in either storage, processing or transit. Without data integrity, the data can not be trusted to be accurate [6]. Available systems are those which are operational and accessible to those who are authorized to do so, when required to be [26].

Data confidentiality and privacy concerns within the crowdsourcing model involve both the protection of private personally identifying information (PII) of those participating, as well, as safeguarding sensitive intellectual property. The unauthorized sharing of crowd member’s personal information, either internally or externally can lead to legal or regulatory penalties, as well as reputation harm. [35]. Sensitive information beyond member PII can also be subject to attack and exfiltration which could result in loss of stakeholder trust, financial implications, and possible penalties [31]. Care is necessary to ensure controls are in place to protect sensitive information based upon ethical policy guidance and industry best practices [36]. Maintaining data integrity within crowdsourcing efforts can be problematic with many examples involving participant’s actively being incentivized to participate in unethical behavior. Through the placement of false information within a crowdsourced event, outcomes can be affected such as the swaying of consumer behavior from targeted bad reviews, the rerouting of human traffic through the input of inaccurate traffic or geographic data to crowdsourced systems, through prank activity to cause harm to others or changing other’s crowdsourcing competition entries to alter the outcome [25].

### 1.4 Research Purpose

As crowdsourced and open innovation initiatives are continuing to grow in popularity, scope and global reach, it is imperative to consider the ethical implications for both the participants, and those who are being served by the project. Privacy in one of the key cybersecurity concerns for participants, as well as ensuring data collected is processed and safeguarded according to industry and regulatory standards. The development of a strength-of-cybersecurity policy taxonomy as related to engineering crowdsourcing is the primary goal of this effort, with the taxonomy scope limited to companies that sponsor crowdsourcing initiatives which have expressed privacy or ethical policies which are available for view through their on-line content.

## 2.0 Methodology

A taxonomy provides a beneficial perspective for the analysis of phenomenon and the relationships between them which can be extended to the evaluation of ethical concepts in crowdsourcing [18]. The development of a taxonomic classification for linking ethical cybersecurity practices into engineering crowdsourcing initiatives requires identification of cybersecurity practices through privacy statements, as well as comparing this to established engineering ethics. A multi-step process was employed to provide a methodic approach to the determination of relevant cybersecurity practices within common crowdsourcing enterprises which includes scope determining and planning, data collection and analysis, taxonomic data classification and the model creation as depicted in Figure 1.

In Step 1, the determination of the research scope and research plan was completed. The definition of study goals with scoping to provide both limitations and ending conditions is key and is central to the planning stage. The development of a strength-of-cybersecurity policy taxonomy as related to engineering crowdsourcing is the primary goal of this effort, with the taxonomy scope limited to companies that sponsor crowdsourcing initiatives. As this is an initial effort to link engineering ethical statements to existing crowdsourcing initiatives, the number of ethical statements and cannons evaluated was limited those presented from National Society of Professional Engineers (NSPE) and the International Information Systems Security Certification Consortium $(ISC)^2$. Similarly, the number of crowdsourcing initiatives considered was limited to six entities to allow the research team to develop the process and taxonomy model. The research plan focused first on key word searches engineering ethics to establish a grounded framework for the evaluation of ethics in the context of crowdsourcing efforts. To select crowdsourced initiatives to be evaluated, keyword searches were included for both crowdsourced and crowdsourcing to establish a pool of potential crowdsourced initiatives and vendors for evaluation. The inclusion criteria for selection was comprised of those initiatives with a web presence that included information regarding their privacy or ethical policies.

Next, Step 2 consisted of data collection and analysis. First, the ethical statements were collected and evaluated for both similarity and divergence, followed by the choice of crowdsourcing initiatives which met the selection criteria requirements. Currently, there are scores of companies in various engineering disciples that sponsor crowdsourcing initiatives, competitions, or events. In this study, over fifty crowdsourcing initiatives and crowdsourcing dedicated vendors were initially evaluated for inclusion into this study, however, many sites evaluated were discarded due to a lack of available policy information regarding privacy or ethics. After the initial evaluation, six of crowdsourcing initiative sites were selected for data collection and subsequent analysis. Data collection consisted of locating the privacy and ethical statement areas of the various crowdsourcing web sites, often found in the support or FAQ sections, then notating the location and content of this section. Analysis of the data consisted of evaluation the privacy and ethical policy statement provided by the crowdsourcing vendors against the selected ethical statements from the NPSE and the $(ISC)^2$.

Following, in Step 3 data classification was performed on the collected data from Step 2. Here the collected data was categorized and aligned to the NPSE and $(ISC)^2$ ethical statements and cannons. Once documented, the taxonomic classification model was created in Step 4. The model was validated using additional crowdsourcing sites which met the inclusion criteria to ensure that as additional crowdsourcing ethical data can be found, the taxonomic model remains flexible to allow for the accommodation of additional data. The model maintenance step provides a method for the taxonomic classification to expand as cybersecurity challenges increase, in tandem with ever evolving crowdsourcing and engineering practices.

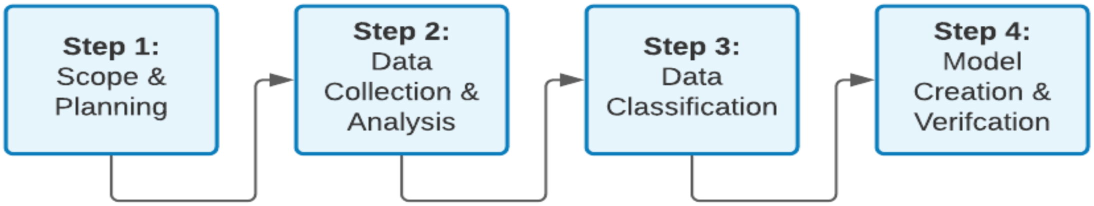

Figure 1. Research Methodology

## 3.0 Taxonomic Classification

The taxonomic classification was prepared through the evaluation of selected crowdsourcing or open innovation sites which had privacy or ethical statements which supported the NPSE and the (ISC)$^2$ ethical standards. The project name and high-level description was provided, with participant recruitment strategy, privacy statement evaluation and ethical considerations. As part of the ethical consideration, a brief description of the either explicitly stated ethical practices was supplied or the implicit ethical goals such as serving the community and doing no harm. Additionally, the NPSE and (ISC)$^2$ ethical standards which best addressed the stated or implied organizational ethics were enumerated for each entry as described in Table 1.

Table 1. Crowdsourced Project, Privacy and Ethics Taxonomic Classification

| Project Name & Description | Recruitment | Privacy Statement | Engineering Ethics |
|---|---|---|---|
| Dell Technologies<br>www.delltechnologies.com/ Crowdsourced Supercomputing: Folding@Home. Crowdsourced computing for genetic studies (Covid, Ebola, etc). [7] | Through Dell and other vendor partners. Open solitication on social media groups. [7] | Account is identified by user choice and PII is not shared, nor is location shared. Email address given is not shared on site or externally. [7] | Folding@Home provides specific instructions as to ethical behavior in conduct for participating in their crowdsourcing effort. [7] NSPE-5, NSPE-6, (ISC)2-1, (ISC)2-2 |
| Ennomotive<br>https://www.ennomotive.com Crowdsourced engineering competition and innovation vendor [9] | Through the Enmotive site. Open solitication on social media groups.[9] | Ennomotive's privacy statement indicates data is only collected and processed for explicit and legitimate purposes. Additionally, Ennomotive provides safeguards for participant PII. [9] | Ennomotive provides no specific ethical directives, although projects which sponsor common good are featured prominently. [9] NSPE-1, NPSE-6, (ISC)2-1, (ISC)2-2 |
| Innocentive<br>https://www.innocentive.com/ Innocentive is part of Wazoku and abides by Wazoku's privacy requirements. Particpants can engage in various for-profit and non-profit open innovation / crowdsourcing initiatives. Wazoku is crowdsourcing / open innovation management software vendor. [15,32] | Directly with Innocentive Challegne or through one of its collabortive partners for either profit or non-profit endevors.[15,32] | Innocentive/Wazoku provides a comprehsive privacy policy consistent with EU's GDPR regulations, with provisions for California (CCPA) and Nevada residents.[15,32] | Innocentive provides contracting for IP specifc to each challenge, verifies solutions and awards monetary compensation as applicable. "Accountable" is one of Wazoku's core company values.[15,32] NPSE-1, NSPE-4, NSPE-6, (ISC)2-1, (ISC)2-2, (ISC)2-3 |
| IDEO - OpenIDEO<br>www.openideo.com/<br>OpenIdeo is an initiative within the IDEO corporation focused on soloving world problems via open innovation and crowdsourcing. [34] | Directly from the OpenIDEO site and through OpenIDEO working innovation chapters. [34] | IDEO complies with the EU-US Privacy Shield Framework and California CCPA Privacy requirements [34] | OpenIDEO provides no direct specific ethical statement, however their open innovation challenges support global issues such as education in developing countries, sustainability projects and woman's health. [34] NPSE-1, NSPE-4, NSPE-6, (ISC)2 -1, (ISC)2 -2, (ISC)2 -3 |
| Humanitarian OpenStreetMap Team<br>www.hotosm.org/<br>The Humanitarian OpenStreetMap Team (HOT) is an internation team focused on harnessing crowdsouced team for mapping data to promote humanitarian action and community development. [13] | Directly from the HOT site and through social media.[13] | HOT supplies a comprehensive privacy statement with information on what data is collected, how it is used, processed and safeguarded. [13] | HOT provides no direct specific ethical statement, however they do validate the mapping data provided by volunteers to ensure accuracy. Mapping projects support lity projects and woman's health. [13] NPSE-1, NSPE-4, NSPE-6, (ISC)2-1, (ISC)2-2, (ISC)2-3 |
| United States Government Challenge<br>www.challenge.gov/about/<br>The United State's governmental program through the GSA engages citizens to source innovative ideas and foster an innovation culture within their own organization and from its citizens. [1] | Directly from the challenge.gov site and from other internal governmental agencies. [1] | The US Challenge.gov program does not collect personal information when the website is visited unless one voluntarily provides that information. Privacy for this site is maintained as to the same level as the US GSA privacy requirements. [1] | Challenge.gov provides no direct specific ethical statement, however they offer numerous challenges which support engineering, health and educational inititives which are sponored by various agencies. [1] NPSE-1, NSPE-2, NSPE-4, NSPE-6, (ISC)2-1, (ISC)2-2, (ISC)2-3 |

## Discussion

Many organizations have crowdsourced or open innovation initiatives to support improvements in their products, social improvements, or for-profit endeavors as vendors for open innovator project management. In this study, six crowdsourcing and open innovation organizations were evaluated and categorized for their privacy statements, recruitment methods and ethical standards. As privacy is one key issues within cybersecurity of crowdsourced and open innovation efforts, privacy statements for each initiative were evaluated. One of the primary challenges for this effort was the lack of consistency of privacy statement location, as well as the consistency of format and content. Some of the crowdsourced sites had limited privacy information and were discarded from consideration. Within the six open innovation and crowdsourced initiatives evaluated, while privacy statements could be found, again there was significant variance as to the content and level of completeness. Open innovation sites located within the European Union or those who dealt with citizens in California in the United States had the most complete privacy data as they were required to adhere to the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). Another issue of cybersecurity issue of data integrity was addressed by the Innocentive, as part of their service, they state they validate the participant solutions prior to acceptance and the Humanitarian OpenStreetMap Team (HOT) which has a separate map validation team which oversees the accuracy input crowdsourced map data.

The ethical standards were evaluated against collected ethical standard statements from both the National Society of Professional Engineers (NSPE) and the International Information Systems Security Certification Consortium (ISC)$^{2.}$ Within those open innovation and crowdsourced sites evaluated, ethical statements were sparser and explicit statements regarding ethical standards were more difficult to find. Only Dell Technologies/Folding@Home and Emmotive provided ethical guidance statements, while the other sites implied ethical standards through providing initiatives which served the community through projects which supported humanitarian issues.

## Limitations and Future Work

As this was an initial attempt to provide a taxonomic view of crowdsourced and open innovation organizational perspectives on privacy, recruitment and engineering ethics, a limited number of these organizations were selected for evaluation. The goal of this research was to select organizations for evaluation that reflected an overview of various types and from differing regions. With the crowdsourcing and open innovation market continuing to expand in size, complexity of project and area of reach, there is significant opportunity for further research into this segment and the investigation of selected crowdsourcing industry silos or specific ethical concern.

## Conclusion

Crowdsourcing and open innovation initiatives continue to be popular methods to engage a large number of people to solve various levels of complex problems. While providing a successful methodology for undertaking a vast variety of engineering and humanitarian issues which harnesses the imagination and talent of people, ethical and security concerns must be addressed to ensure both the participants and those receiving the services are kept from harm. Crowdsourced and open innovation initiatives provide significant opportunities for various people who perhaps would not have the ability to contribute to interesting and projects which benefit humanity at large. Within collegiate engineering curriculum, ethical practices are outlined and reinforced through various upper-level course work specific to each branch of study. The ability to tailor the crowdsourced or open innovation tasks to the student's skill level and interests, provides an opportunity for the student to gain confidence professionally while contributing to a larger project. The participation of students in humanitarian-based engineering crowdsourcing efforts, allows the student to both hone their skills, as well as practice some of the NPSE ethical obligations in preparation for their professional career.

In this study, crowdsourced and open innovation organizations were evaluated for their stated and implied privacy and ethical standards. A project methodology was proposed which outlined the steps which were used in the creation of the taxonomic model which included the determination of the scope and planning step, followed by data collection and analysis step, then the categorization of the data and building of the taxonomy. Over fifty organizations were initially considered, but many of these sites had limited or difficult to find privacy statements so they were excluded from secondary consideration. Six organizations, representing multiple regions and focus areas were selected for the taxonomic categorization. These privacy standards, recruitment methods and ethical statements were evaluated against the National Society of Professional Engineers (NSPE) relies on the "Code of Ethics for Engineers" and the $(ISC)^2$ ethical cannons and this information was categorized and presented in a taxonomic model.

While this is an initial effort, several challenges emerged as to the collection of the privacy and ethical statement data. This information is applied in a non-standard manner on every organization's web site considered and in highly dissimilar formats and content. This makes it difficult for the participant to easily evaluate their rights and organization's provided safeguards. Additionally, direct statements as to ethical practices, policies or standards were often not present, and required significant work to ascertain them if they were at all available. Implicit ethical behavior was expressed through the selection of crowdsourced projects which emphasized humanitarian-based projects.

**References**

[1] *About.* About | Challenge.gov. (n.d.). Retrieved October 5, 2021, from https://www.challenge.gov/about/.

[2] Brabham, D. C. (2008). *Crowdsourcing as a Model for Problem Solving: An Introduction and Cases*. https://doi.org/10.1177/1354856507084420

[3] Cancialosi, C. (2020, July 31). *The Future of Crowdsourcing*. Forbes. Retrieved October 11, 2021, from https://www.forbes.com/sites/chriscancialosi/2019/11/21/the-future-of-crowdsourcing/?sh=4de8a268434b.

[4] Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & Sweetnam, J. (2020). *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*. https://doi.org/10.6028/nist.sp.1800-25

[5] *Crowdsourcing is not new - the history of crowdsourcing (1714 to 2010).* DesignCrowd. (n.d.). Retrieved October 11, 2021, from https://blog.designcrowd.com/article/202/crowdsourcing-is-not-new--the-history-of-crowdsourcing-1714-to-2010.

[6] *Cybersecurity and IT security certifications and training: (ISC*)². Cybersecurity and IT Security Certifications and Training | (ISC)². (n.d.). Retrieved October 11, 2021, from https://www.isc2.org/.

[7] *Digital Transformation - IT & Workforce Solutions.* Dell Technologies US. (n.d.). Retrieved October 6, 2021, from https://www.delltechnologies.com/en-us/index.htm.

[8] Estellés-Arolas, E., & González-Ladrón-de-Guevara, F. (2012). *Towards an integrated crowdsourcing definition.* Journal of Information science, 38(2), 189-200.

[9] Ennomotive. (n.d.). *Open Innovation Hub for Companies, Startups, and Experts*. Retrieved October 10, 2021, from https://www.ennomotive.com/.

[10] Githui, D. M. (2012). Ethical issues in the construction industry in Kenya: A critical analysis of the professional conduct in engineering technology management.

[11] *Global $135 Mn Crowdsourced Security Markets to 2024 - Growth of IoT to Increase the Need for Crowdsourced Security Services - ResearchAndMarkets.com*. (2019, October 17). Www.businesswire.com.

[12] Howe, J. (2006, June 1). The rise of Crowdsourcing. Wired. Retrieved October 11, 2021, from https://www.wired.com/2006/06/crowds/.

[13] *Humanitarian openstreetmap team: Home.* Humanitarian OpenStreetMap Team | Home. (n.d.). Retrieved October 2, 2021, from https://www.hotosm.org/.

[14] *IEEE code of Ethics*. IEEE. (2020). Retrieved October 4, 2021, from https://www.ieee.org/about/corporate/governance/p7-8.html.

[15] *InnoCentive.* (2021, September 15). Retrieved October 8, 2021, from https://www.innocentive.com/.

[16] *Issa code of ethics - information systems security association*. (n.d.). Retrieved September 29, 2021, from https://www.members.issa.org/page/codeofethics.

[17] Kietzmann, J. H. (2017). Crowdsourcing: A revised definition and introduction to new research. *Business horizons*, *60*(2), 151-153.

[18] Kocsis, D., & de Vreede, G. J. (2016). Towards a taxonomy of ethical considerations in crowdsourcing.

[19] Maxwell. J. C. (2008). *Ethics 101 what every leader needs to know*. Hachette Nashville.

[20] Merriam-Webster. (n.d.). *Unethical*. Merriam-Webster. Retrieved October 2, 2021, from https://www.merriam-webster.com/dictionary/unethical#:~:text=%3A%20not%20conforming%20to%20a%20high,practices%20immoral%20and%20unethical%20behavior.

[21] Nadikattu, R. R. (2020). New Ways of Implementing Cyber Security to Help in Protecting America. *Journal of Xidian University*, *14*(5), 6004-6015.

[22] National Society of Professional Engineers. (2021). *NSPE Code of Ethics for Engineers*. Code of Ethics | National Society of Professional Engineers. Retrieved October 4, 2021, from https://www.nspe.org/resources/ethics/code-ethics.

[23] NIST (n.d.). *privacy - Glossary | CSRC*. Csrc.nist.gov. Retrieved October 6, 2021, from https://csrc.nist.gov/glossary/term/privacy

[24] Qadir, S., & Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. Journal of Information Security, 7(3), 185-194.

[25] Rinta-Kahila, T., & Soliman, W. (2017). Understanding crowdsourcing: the different ethical logics behind the clandestine industry of deception. In *ECIS 2017: Proceedings of the 25th European Conference on Information Systems, Guimarães, Portugal, June 5-10, 2017, ISBN 978-989-20-7655-3*. European Conference on Information Systems.

[26] Ross, R. S. (2014). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*: https://doi.org/10.6028/nist.sp.800-53ar4

[27] Ross, R., McEvilley, M., & Oren, J. C. (2018). *Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems*, volume 1. https://doi.org/10.6028/nist.sp.800-160v1

[28] *Rules & Policies*. (n.d.). Folding@Home. Retrieved October 8, 2021, from https://foldingathome.org/support/faq/rules-policies/?lng=en

[29] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

[30] Sandhu, R. S. (1993, September). On Five Definitions of Data Integrity. In *Proceedings of the IFIP WG11. 3 Working Conference on Database Security VII* (pp. 257-267).

[31] Schlagwein, D., Cecez-Kecmanovic, D., & Hanckel, B. (2019). Ethical norms and issues in crowdsourcing practices: A Habermasian analysis. *Information Systems Journal*, *29*(4), 811-837.

[32] Simon. (2021, April 7). Wazoku Privacy policy. Wazoku. Retrieved October 8, 2021, from https://www.wazoku.com/privacy

[33] Shah, R. K., & Alotaibi, M. (2018). A Study of Unethical Practices in the Construction Industry and Potential Preventive Measures. *Journal of Advanced College of Engineering and Management*, *3*, 55. https://doi.org/10.3126/jacem.v3i0.18905

[34] *Social Impact powered by design thinking.* OpenIDEO. (n.d.). Retrieved October 3, 2021, from https://www.openideo.com/.

[35] Wolfson, S. M., & Lease, M. (2011). Look before you leap: Legal pitfalls of crowdsourcing. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1-10.

[36] Xia, H., & McKernan, B. (2020). Privacy in Crowdsourcing: a Review of the Threats and Challenges. *Computer Supported Cooperative Work (CSCW)*, *29*(3), 263-301.

[37] Veach, C. M. (2006). There’s no such thing as engineering ethics. *Leadership and Management in Engineering*, *6*(3), 97–101. https://doi.org/10.1061/(asce)1532-6748(2006)6:3(97)