ComplianceNet

Working Paper Series *Article 7; 2019*

Corporate Codes and Unethical Coding

Jonathan J. Rusch
Georgetown University Law Center

Working Paper

ComplianceNet is an international network of scholars from across the social and behavioral sciences who study compliance, broadly defined as the interaction between rules and individual and organizational behavior. The network publishes a working paper series that offers the latest work in this field. The papers are unpublished drafts or pre-published versions of publications. Submissions can be sent to the editors, Melissa Rorie, melissa.rorie@unlv.edu, Benjamin van Rooij, bvanrooij@law.uci.edu, and Yuval Feldman, Yuval.Feldman@biu.ac.il

ComplianceNet.org

Corporate Codes and Unethical Coding

Jonathan Rusch

Abstract

In recent years, various situations have come to light in which software engineers have written or acquired code that allows individuals to engage in practices that are unethical, if not illegal. For example, in the Volkswagen emissions scandal, Volkswagen acquired engine-management software from a legitimate third-party supplier for use during emissions testing, knowing that using it in publicly sold vehicles was illegal, but used it to create "defeat devices" to cheat on compliance with emissions standards. More recently, Google and Apple have received substantial criticisms for hosting Absher, a Saudi-Arabian Government-created app that allows male guardians to control where women may travel or be informed when a woman swipes a passport. This paper will discuss the extent to which general corporate codes of ethics and conduct, as well as software industry-specific codes of ethics, fail to address the creation, acquisition, or use of software that has a primary function of engaging in unethical or illegal conduct (e.g., violating human rights standards or national legislation), and recommend why and how those codes should be revised to proscribe creating, acquiring, or using such software.

Keywords: code of ethics, technology, software, human rights, corporate compliance

Introduction

For more than half a century, computing professionals have recognized that computing design and operations have ethical ramifications.[1] Associations of computing professionals have adopted codes of conduct and ethics that reflect broad commitment to ethical precepts, universities have included computer ethics courses in their curricula, and academicians have written computer- and information ethics textbooks and held academic conferences in which computing ethics have been extensively discussed.[2] In addition, leading technology companies have adopted codes of ethics that broadly reflect their commitment to ethical conduct.[3]

Even after five decades of research and discussion, however, "there is no common understanding of key components of the ethics of computing as perceived and put in practice by the communities of technical scholars and practitioners."[4] One of those key components is a failure to address the practice of writing and distribution of certain types of software, or creating and distributing software/hardware systems, that directly further or facilitate conduct that is commonly recognized as illegal or violative of human rights.

In recent years, a number of situations have come to light in which software engineers have written or acquired code that, given its nature or purpose, clearly allows the ultimate users of that code to engage in practices that are illegal or that significantly impinge on human rights:

- In the Volkswagen emissions scandal, Volkswagen acquired engine-management software from a legitimate third-party supplier for use during emissions testing, knowing that using it in publicly sold vehicles was illegal, but used it to create "defeat devices" to cheat on compliance with emissions

---

1 *See, e.g.*, Bernd Carsten Stahl, Job Timmermans, and Brent Daniel Mittelstadt, *The Ethics of Computing: A Survey of the Computing-Oriented Literature*. 48 ACM COMPUT. SURV. 55:1 (February 2016), https://www.researchgate.net/publication/295683999_The_Ethics_of_Computing.

2 *See id.* 55:5.

3 *See, e.g., infra* pp. 7-10.

4 Bernd Carsten Stahl, Job Timmermans, and Brent Daniel Mittelstadt, *supra* note 1, at 55:1.

standards.[5] The use of such software extended to multiple automakers. Recently, for example, Porsche (a Volkswagen subsidiary), agreed to pay a €535 million ($598 million) fine "for the use of software to hide the true level of harmful emissions by diesel cars."[6]

- Google and Apple have been the targets of substantial criticism for hosting Absher, a Saudi-Arabian Government-created app that allows male guardians to control where women may travel or be informed when a woman swipes a passport.[7]

- The Chinese government has created and implemented a comprehensive surveillance system in Xinjiang province to track and monitor the Uighur minority population there. One component of the system is "a vast, secret system of advanced facial recognition technology" that constitutes "the first known example of a government intentionally using artificial intelligence for racial profiling."[8] The technology, "which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review."[9]

  Another component of that system, according to a recent Human Rights Watch report, is a mobile phone app "used by officials to connect to a policing programme which aggregates data about people and flags up those deemed a threat."[10] This app reportedly "can track an individual's electricity use, raise an alert if someone other than the registered owner fills up a vehicle with petrol and monitor internet use."[11] Moreover, the surveillance system of which the app is only one small part "allows authorities to identify potential troublemakers by their behaviour, using a combination of CCTV cameras, GPS devices that are required on cars, and neighbourhood snitches. . . . Those identified may be restricted in their daily movements or even sent to a detention camp."[12] By one recent estimate, as many as one million Uighurs are now held in detention camps.[13]

- Most recently, media reports disclosed that spyware created and marked by an Israeli technology firm, the NSO Group, can exploit a security flaw in the popular messaging app WhatsApp "to insert malicious code and steal data from an Android phone or an iPhone simply by placing a WhatsApp call, even if the victim did not pick up the call."[14] While the NSO Group's website states that the company "creates technology that helps government agencies prevent and investigate terrorism and crime to save

---

[5] *See* Darden Business Publishing, University of Virginia, The Volkswagen Emissions Scandal (revised February 3, 2017), https://www.americanbar.org/content/dam/aba/events/criminal_justice/2018/Ethical_Guidance_VW_Emission_Scandal.pdf.
[6] *Porsche fined 535 million euros over diesel scandal*, DEUTSCHE WELLE, May 7, 2019, https://www.dw.com/en/porsche-fined-535-million-euros-over-diesel-scandal/a-48636072.
[7] *See* Hamza Shaban, *Critics call on Apple and Google to shut down Saudi app that can restrict women's travel*, WASHINGTON POST, February 12, 2019, https://www.washingtonpost.com/technology/2019/02/12/human-rights-groups-call-apple-google-review-saudi-app-that-can-restrict-womens-travel/?utm_term=.dd17e2d92c1f.
[8] Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, NEW YORK TIMES, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[9] *Id.*
[10] Didi Tang, *Chinese app tracks every move that Muslims make*, THE TIMES, May 3, 2019, https://www.thetimes.co.uk/edition/world/chinese-app-tracks-every-move-that-muslims-make-0dhz0dpzl.
[11] *Id.*
[12] *Id.*
[13] *See* Paul Mozur, *supra* note 8.
[14] Nicole Perlroth and Ronen Bergman, *Israeli Firm Tied to Tool That Uses WhatsApp Flaw to Spy on Activists*, NEW YORK TIMES, May 13, 2019, https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html.

> thousands of lives around the globe,"[15] security researchers found that the NSO spyware, Pegasus, exploited the WhatsApp security hole "to target a London lawyer who has been involved in lawsuits that accuse NSO Group of providing tools to hack the phones of Omar Abdulaziz, a Saudi dissident in Canada; a Qatari citizen; and a group of Mexican journalists and activists."[16]

This paper will examine three leading nonprofit computing professionals' and business associations' code of ethics, as well as two examples of information technology companies' codes of ethics. For both types of codes, it will identify and discuss whether those codes fail to state that the creation, acquisition, distribution, or use of, or facilitating or supporting the use of, software or systems whose purpose or necessary effect is to further or facilitate conduct that is illegal or violates human rights norms is unethical and prohibited under all circumstances. It will then make two recommendations for revising codes of ethics to prohibit creating, acquiring, distributing, using, or facilitating or supporting the use of such software and systems.

I. Current Codes of Ethics

For many companies and professional organizations today, codes of ethics[17] are not just desirable as a means of expressing corporate values and expectations, but essential to demonstrating to regulatory and enforcement authorities that those companies are committed to maintaining a culture of compliance.[18] For example, under Section 406 of the Sarbanes-Oxley Act and implementing regulations, publicly traded companies are required to adopt a code of ethics applicable to specific senior officers.[19] Those regulations define a 'code of ethics" to mean "written standards that are reasonably designed to deter wrongdoing" and to promote various behaviors by senior executives, such as "[h]onest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships."[20]

All compliance-related policies and codes of ethics, of course, must strike a balance between clarity and concision.[21] No corporate policy or code of ethics can provide for every contingency in everyday business without reaching interminable lengths. Nor should it be so vague and generic that it offers no meaningful guidance on ethical behavior. But every code of ethics must be clear about what conduct it clearly prohibits under any circumstances, such as bribery or insider trading.[22]

For those reasons, any organization's first step in drafting a code of ethics must be "deciding what values are important to it and what lines it won't cross."[23] For example, one business school professor who advises clients

---

15 NSO Group, https://www.nsogroup.com/ (accessed May 14, 2019).

16 Nicole Perlroth and Ronen Bergman, *supra* note 14.

17 Because associations and companies vary between labeling their ethics-related codes as codes of conduct, ethics, or conduct and ethics, this paper will hereafter refer to all such codes in this paper as "codes of ethics."

18 *See* Josh Spero, *How to Write a Code of Ethics for Business*, inc.com, August 24, 2010, https://www.inc.com/guides/how-to-write-a-code-of-ethics.html.

19 17 C.F.R. §229.406(a).

20 *Id.* §229.406(b).

21 *See, e.g.*, Michael Volkov, *Writing Effective and Clear Compliance Policies*, CORRUPTION, CRIME & COMPLIANCE, February 10, 2016, https://blog.volkovlaw.com/2016/02/writing-effective-clear-compliance-policies/.

22 *See, e.g.*, Coca-Cola Company, Code of Business Conduct at 29-30 (revised February 12, 2018) (bribery and insider trading), https://www.coca-colacompany.com/content/dam/journey/us/en/private/fileassets/pdf/2018/Coca-Cola-COC-External.pdf; Starbucks, Standards of Business Conduct (gifts and entertainment), https://livingourvalues.starbucks.com/en-us/business-practices.

23 *See* Josh Spero, *supra* note 13.

asks them, "'What are the things you would never do at this company to get a client, to keep a client, to make sure you met your numbers for the quarter?' Just thinking through that sets the framework for the code'."[24]

With those basic precepts in mind, this section will review the provisions of three codes of ethics by leading information-technology professional and business associations, and of various technology companies' codes. It will focus on whether those codes make clear that computing professionals should never engage in actions involving the creation of technology – including computer hardware and software – whose primary purpose is to further or facilitate criminal activity or human rights violations.

A. Professional Associations' Codes of Ethics

1. Association for Computing Machinery

Arguably the most detailed non-corporate code of ethics by and for computing professionals is the Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct (Code). The ACM, which describes itself as "the world's largest educational and scientific computing society,"[25] is a nonprofit organization of nearly 100,000 computing educators, researchers, and professionals.[26] The ACM Code, which the ACM revised in 2018, has two stated purposes: (1) "to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way"; and (2) to serve "as a basis for remediation when violations occur."[27]

The ACM Code has two principal components: (1) "principles," which the ACM states are "formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration; and (2) guidelines that supplement each principle and "provide explanations to assist computing professionals in understanding and applying the principle."[28] Similar to corporate codes of conduct and ethics, the ACM Code's principles are broadly framed to reflect the ACM's basic values (e.g., "Contribute to society and to human well-being,"[29] "Avoid harm,"[30] and "Be honest and trustworthy"[31]).

In general terms, the ACM Code has very few outright prohibitions on conduct by computing professionals. The guidelines for Principle 1.3 state that "[m]aking deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code."[32] Under Principle 1.4, "1.4 Be fair and take action not to discriminate," the guidelines specifically state: "Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code." Those guidelines, however, do not address situations in which a computing professional is tasked with writing software, or approving the sale of software, that would

---

[24] *Id.*
[25] Association for Computing Machinery, About ACM, https://www.acm.org/about-acm (accessed May 7, 2019).
[26] See Association for Computing Machinery, About the ACM Organization, https://www.acm.org/about-acm/about-the-acm-organization (accessed May 7, 2019).
[27] Association for Computing Machinery, ACM Code of Ethics and Professional Conduct, https://www.acm.org/code-of-ethics (accessed May 7, 2019).
[28] *Id.*
[29] *Id.*, Principle 1.1.
[30] *Id.*, Principle 1.2.
[31] *Id.*, Principle 1.3.
[32] *Id.*

have the primary purpose or necessary effect of allowing the software's user (rather than the coder) to engage in prejudicial discrimination against others.

Other principles and guidelines indicate that computing professionals should be mindful of the effects of their work on individuals. For example, Principle 3.1's guidelines generally state that "[p]eople—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing."[33] The guidelines for Principle 1.2, "Avoid harm," make clear that "harm" means "negative consequences, especially when those consequences are significant and unjust," including "unjustified physical or mental injury."[34] Those guidelines include the following admonitions:

> Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified. In either case, ensure that all harm is minimized.[35]

Those admonitions, however, provide no guidance on what a professional covered by the Code should do if he or she is asked to perform a task, such as coding, in which there is no ethical justification for the harm – as would be the case if the software is meant to give false information to others in furtherance of a crime (e.g., the emissions-cheating software in the Volkswagen case) or to further or facilitate human-rights violation (e.g., the Absher software and the Chinese facial-recognition technology deployed to monitor Uighur people) – and no way to minimize the harm.

2. Institute of Electrical and Electronics Engineers

Another leading computing-professionals' nonprofit organization is the Institute of Electrical and Electronics Engineers (IEEE). The IEEE, which calls itself "the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity,"[36] boasts more than 422,000 members in more than 160 countries.

The IEEE Code of Ethics, at only 369 words, is far shorter than the ACM Code. It states that the members of the IEEE "hereby commit ourselves to the highest ethical and professional conduct and agree" to ten generic principles.[37] Only one of those principles, Principle 4, involves complete prohibition of certain conduct (i.e., Principle 4, "reject[ing] bribery in all its forms." Other principles, like the ACM Code's principles, broadly reflect the IEEE membership's core values:

- **Principle 1** - "to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment."[38] These broad concepts do not define what constitutes "ethical design," or explain to whom an IEEE member would disclose the potential or planned use of software to further a crime or violate a minority group's human rights (or what recourse that member

---

[33] *Id.*
[34] *Id.*, Principle 1.2.
[35] *Id.*
[36] IEEE, IEEE at a Glance, https://www.ieee.org/about/today/at-a-glance.html?WT.mc_id=ab_lp_qui (accessed May 8, 2019).
[37] IEEE, IEEE Code of Ethics, https://www.ieee.org/about/corporate/governance/p7-8.html (accessed May 8, 2019).
[38] *Id.*

would have should the person or organization to which the member makes that disclosure reject or ignore the disclosure and decide to sell or distribute that software).

- **Principle 5** - "to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression."[39] As with the ACM Code, this language does not provide guidance on what a software engineer should do if he or she is not engaging in discrimination, but creating software or systems that the buyer plans to use to conduct systematic and invidious discrimination against others.

3. Responsible Business Alliance Code of Conduct

A third code of ethics, which indirectly reflects a measure of consensus among technology companies, is the Responsible Business Alliance (RBA) Code of Conduct.[40] In that Code, the RBA (formerly the Electronic Industry Citizenship Coalition) states that it "establishes standards to ensure that working conditions in the electronics industry or industries in which electronics is a key component and its supply chains are safe, that workers are treated with respect and dignity, and that business operations are environmentally responsible and conducted ethically."[41]

With regard to ethical conduct, the RBA Code specifically states that "[p]articipants shall have a zero tolerance policy to prohibit any and all forms of bribery, corruption, extortion and embezzlement," and that "[b]ribes or other means of obtaining undue or improper advantage are not to be promised, offered, authorized, given or accepted."[42]

In addition, the Code contains one specific human rights-related provision, stemming from widespread recognition that "[a]rmed groups in the Democratic Republic of the Congo have committed severe human rights abuses, including sexual violence, and reportedly profit from mining and trade in tungsten, gold and other 'conflict minerals' found in the region."[43] The Code states that "[p]articipants shall have a policy to reasonably assure that the tantalum, tin, tungsten and gold in the products they manufacture does not directly or indirectly finance or benefit armed groups that are perpetrators of serious human rights abuses in the Democratic Republic of the Congo or an adjoining country."[44] That latter provision, however, addresses human-rights concerns only with regard to the acquisition of conflict minerals, and not human rights violations or criminal actions that are foreseeable consequences of the sales of technology products or services.

B. Information Technology Industry Codes of Ethics

In part because commercial organizations are directly at risk if they violate civil or criminal statutes, companies generally appear attentive to specifying for employees, via their codes of ethics, which kinds of conduct are prohibited under any circumstances. The extent to which they do so, however, varies substantially within the technology sector.

---

[39] *Id.*

[40] *See* Responsible Business Alliance, Responsible Business Alliance Code of Conduct, Version 6.0 (2018), https://www.responsiblebusiness.org/media/docs/RBACodeofConduct6.0_English.pdf.

[41] *Id.* 1.

[42] *Id.* 10.

[43] GENERAL ACCOUNTABILITY OFFICE, COMPANY REPORTS ON MINERAL SOURCES IN 2017 ARE SIMILAR TO PRIOR YEARS AND NEW DATA ON SEXUAL VIOLENCE ARE AVAILABLE, Report No. GAO-18-457 (June 18, 2018), https://www.gao.gov/products/GAO-18-457.

[44] Responsible Business Alliance, *supra* note 40, at 11.

While there are numerous technology companies whose codes of ethics could be reviewed, this section will concentrate on the codes of ethics of two leading companies, Intel and Microsoft. [The selection of companies for this review was nonrandom, and based in part on a]May 2019 list by *Investopedia* of the world's top 10 leading software companies.[45]

1. Intel Corporation

The Intel Code of Conduct[46], like many other corporate codes, is organized around the company's vision and core values.[47] Unlike many companies, it devotes an entire section to the topic of "Follow the Letter and the Spirit of the Law."[48] In that section, it states generally that "as a global company Intel must comply with the laws of the many countries in which it does business" and that "[w]e also must act in a manner that upholds the intent and the spirit of the law."[49]

Furthermore, with regard to multiple areas of legal compliance, the Intel Code includes specific prohibitions on employee conduct:

- **Antitrust Laws**: "[W]e must not . . . [c]ommunicate with any competitor relating to price, any term that affects pricing, or production levels, . . . [d]ivide or allocate customers or markets, . . . [a]gree with a competitor to boycott another business, or . . . [p]ut inappropriate conditions on purchases or sales."[50]
- **Bribery and Anti-Corruption**: "Intel strictly prohibits all forms of bribery. . . . We must never offer or accept bribes or kickbacks and must not participate in or facilitate corrupt activity of any kind. . . . We do not make facilitation payments on behalf of intel to ay government official."[51] In addition, this antibribery provision "also applies to third parties who provide services or act on Intel's behalf, such as suppliers, agents, contractors, consultants and distributors."[52]
- **Import and Export Compliance**: Because "[w]e have a responsibility to comply with [import and export] laws and regulations[,] . . . we must clear all goods through customs and must not . . . [p]roceed with a transaction if we know that a violation has occurred or is about to occur; [t]ransfer controlled software and technology unless appropriate authorizations are obtained; or [a]pply an inappropriate monetary value to goods and services."[53]

The Intel Code, however, does not include a broader statement that the company is opposed to participating in any way in the creation, acquisition, distribution, or use of software or hardware whose purpose or necessary effect is to violate the law or human rights.

---

45 *See* Shobhit Seth, *World's Top 10 Software Companies*, INVESTOPEDIA (updated May 5, 2019), https://www.investopedia.com/articles/personal-finance/121714/worlds-top-10-software-companies.asp. Because many technology companies now offer a variety of software and hardware products and solutions, for purposes of this paper it seems artificial to try to separate the reviewed companies into separate categories of software and hardware.

46 *See* Intel, Intel Code of Conduct (January 2019), https://www.intel.com/content/www/us/en/policy/policy-code-conduct-corporate-information.html.

47 *See id.* 2.

48 *See id.* 7.

49 *Id.*

50 *Id.* 8.

51 *Id.*

52 *Id.*

53 *Id.* 9.

2. Microsoft

Microsoft's Standards of Business Conduct[54] is similarly organized around the company's culture and values. The Standards focus on six principal topics:

- **Speaking Up**.[55]

- **Trust with Our Customers**.[56] Under this topic, the Standard specifically state, "Don't Make Improper Payments."[57]

- **Trust with Governments and Communities**.[58] Under this topic, the Standards state, "Respect Laws Around the World," explaining, "We follow the laws and regulations of the U.S. and of all the places where we operate."[59] The Standards also state, "Respect and Promote Human Rights," and declare Microsoft's commitment "to respecting and promoting human rights to ensure that technology plays a positive role across the globe."[60]

- **Trust with Each Other**.[61] Under this topic, the Standards state, "Foster Diversity and Inclusion," explaining in part, "We do not discriminate based on age, ancestry, color, family or medical care leave, gender identity or expression, genetic information, marital status, medical condition, national origin, physical or mental disability, political affiliation, protected veteran status, race, religion, sex (including pregnancy), sexual orientation, or any other characteristic protected by applicable laws, regulations, and ordinances."[62]

- **Trust with Our Investors & the Public**.[63] Under this topic, the Standards contain several statements prohibiting certain conduct. These include:
    - "Don't Trade on Inside Information." The Standards' explanation of this standard include the following statements:
        - "We never buy or sell any securities based on material, nonpublic information.
        - "We do not give someone else (for example, a friend, spouse, or broker) a 'tip' regarding material, nonpublic information.

---

[54] MICROSOFT, ACHIEVE MORE: STANDARDS OF BUSINESS CONDUCT, file:///C:/Users/Jonathan%20Rusch/Downloads/Microsoft%20SBC%20-%20English.pdf (accessed May 29, 2019).
[55] *See id.* 11.
[56] *See id.* 20.
[57] *Id.* 22.
[58] *Id.* 25.
[59] *Id.* 26.
[60] *Id.* 30.
[61] *See id.* 31.
[62] *Id.* 34.
[63] *See id.* 41.

        - "We do not recommend or suggest that anyone else trade in the securities of any company based on material nonpublic information, even if we are not sharing the information itself."[64]
    - Keep Accurate Records and Contracts. The Standards' explanation of this standard includes the statement, "We don't make side agreements or other "off-the-book" arrangements."[65]
    - Protect Confidential Information & Intellectual Property.[66] The Standards' explanation of this standard includes the statement, "We do not use confidential information for non-Microsoft business use, and we maintain confidentiality even if we stop working for Microsoft."[67]

- **Trust with Our Representatives**.[68] Under this topic, the Standards state, "Use Trustworthy Representatives," adding, "We do not pressure partners or resellers to place orders for products or services they do not want or need, or retaliate against them for refusing to do so."[69] The Standards also state, "Treat Gifts, Hospitality, & Travel Responsibly," further specifying:
    - "We never give or accept cash.
    - "We do not solicit gifts, hospitality or travel from third parties, or put them in a position where they feel obligated to provide something in order to do business with us.
    - "We don't ask a representative, like a partner or supplier, to give gifts, hospitality, or travel on our behalf."[70]

Like the Intel Code, however, the Microsoft Standards do not include a broader statement that the company is opposed to participating in any way in the creation, acquisition, distribution or use of software or hardware whose purpose or necessary effect is to violate the law or human rights.

II. Revising Computing Professionals' Codes of Ethics

In the past, many responsible and informed businesspeople would likely have rejected the notion that companies and computing professionals need to include in their codes of ethics a specific statement opposing the making, distribution, or use of software or hardware intended to violate the law or human rights norms. Cases such as the Volkswagen emissions scandal, the Chinese government's Uighur surveillance, and the Pegasus spyware, however, strongly indicate that companies need to recognize and address the ramifications of providing or using software or hardware that furthers criminal conduct or human rights violations.

In addition to the very real compliance risks that such software can create, companies need to recognize the potential for litigation and reputational risks. As one example, NSO, the Israeli company that produces the spyware allegedly used against activists and journalists, is now facing litigation by Amnesty International and other organizations, as well as Israeli citizens, based on their concerns about the ramifications of its uses for surveillance of legitimate advocacy and journalism.[71]

---

64 *Id.* 42.
65 *Id.*
66 *See id.* 47.
67 *Id.*
68 *See id.* 48.
69 *Id.* 50.
70 *Id.* 53.
71 *See* D J Pangburn, *After WhatsApp hack, NSO faces scrutiny from Facebook and UK public pension fund*, FAST COMPANY, May 21, 2019, Dan Sabbagh, *Israeli firm linked to WhatsApp spyware attack faces lawsuit*, THE GUARDIAN, May 18, 2019, https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit.

Two recent reports indicate that this issue is becoming a matter of public concern. Last month, Amazon shareholders offered a resolution that asks Amazon "to prohibit sales of its facial recognition system, called Amazon Rekognition, to government agencies, unless its board concludes that the technology does not facilitate human rights violations."[72] In addition, Novalpina Capital, the United Kingdom private equity fund that holds a substantial stake in the Israeli spyware company, has stated that it will insist on more substantial governance in the light of the WhatsApp controversy.[73] Such developments are likely to become more frequent in the near future.

For these reasons, technology companies and computing-professionals' associations should take the lead in revising codes of ethics to include two specific sets of provisions:

- Specific prohibitions on companies and corporate employees' engaging in development, acquisition, distribution, or use of, or facilitating or supporting use of, software or systems that the company has reason to believe the intended recipient or customer will use to violate criminal laws, civil laws and regulations, or human rights norms; and
- Specific provisions that require employees to report internally (via hotlines, compliance teams, or other identified channels) any efforts to authorize, develop, acquire, issue, distribute, or use software and systems that they have reason to believe the intended recipient or customer will use to violate criminal laws, civil laws and regulations, or human rights laws/norms

Neither set of provisions should impair the ability of any company, government agency, or nonprofit entity to conduct legitimate activities and operations. But both sets are necessary for companies, agencies, and nonprofits to demonstrate their commitment to the rule of law and strengthen their ethical framework for corporate governance.

[72] Natasha Singer, *Amazon Faces Investor Pressure Over Facial Recognition*, NEW YORK TIMES, May 20, 2019, https://www.nytimes.com/2019/05/20/technology/amazon-facial-recognition.html.

[73] *See* Hasan Choudhury, *Israeli spyware firm's British financial backer promises 'transparency' after WhatsApp hack*, TELEGRAPH, May 16, 2019, https://www.telegraph.co.uk/technology/2019/05/15/israeli-spyware-firms-financial-backer-promises-transparency/.