12/8/2018

Richard Rennehan

isec3050-701

Intel’s Ethics and Privacy Policies

Case 2

Contents

[Introduction 2](#_Toc531849835)

[Code of Conduct 3](#_Toc531849836)

[Overview 3](#_Toc531849837)

[Honesty and Law 3](#_Toc531849838)

[Fair Treatment 4](#_Toc531849839)

[Intel’s Guide to Privacy and Protection of Data 6](#_Toc531849840)

[Views on Privacy and Security 6](#_Toc531849841)

[Privacy and Security Implementations 7](#_Toc531849842)

[Intel Corporate Privacy Rules 9](#_Toc531849843)

[Collecting and Using Personal Information 9](#_Toc531849844)

[Audit Protocols 10](#_Toc531849845)

[Complaint Handling Procedure 10](#_Toc531849846)

[Conclusion 12](#_Toc531849847)

[References 13](#_Toc531849848)

# Introduction

According to Ethisphere, Intel was one of the top 124 most ethical companies in the world for 2017 (Jeff Kauflin, 2017). Each company that pays the application fee to apply must complete a detailed 200-question survey explaining their ethics practices (Jeff Kauflin, 2017). The 5 criteria that determines the company’s score from greatest to least include the company’s ethics and compliance program, whether ethics are embedded from top to bottom of the company, corporate citizenship and responsibility, corporate governance, and a combination of leadership, innovation, and reputation (Kauflin, 2017).

Intel’s impact on the IT industry is undoubtedly enormous. For companies looking to make their home in the IT industry, Intel should be a role model for ethics and behavior. This report will cover a brief look at Intel’s code of conduct and privacy policies to understand how Intel handles ethics in the workplace and privacy laws.

# Code of Conduct

Intel’s code of conduct covers numerous topics. The ones most affecting people in the IT industry include company values, responsibilities, conducting business, privacy, and fair treatment of employees. The goal of their code of conduct is to set the standard for how Intel works together to develop and deliver products and how Intel works with customers, suppliers, distributors, and others (Intel, 2018)

Intel’s code of conduct is richly detailed and does a great job at conveying what is expected at the company. It sets a great example for other companies to follow.

## Overview

Intel describes the company as “A Culture of Uncompromising Integrity.” Their vision is: “If it is smart and connected, it is best with Intel.” (Intel, 2018).

The code of conduct reinforces that each employee is responsible for reporting ethical concerns. Each employee should conduct business with honesty and integrity, follow the letter and spirit of the law and treat each other fairly. (Intel, 2018).

## Honesty and Law

To conduct business with honesty and integrity, each employee must communicate respectfully, treat others fairly, act as a responsible corporate citizen, and respect human rights. Intel focuses on achieving business success “in ways that demonstrate respect for people and the planet and upholding the values and high standards of ethics expressed in our Human Rights Principles and our Environment, Health, and Safety Policy.” (Intel, 2018).

To follow the letter and spirit of the law, Intel focuses on “complying with laws of all countries where it does business.” The document places great emphasis on complying with antitrust laws and explaining how to adhere to them. Intel also places emphasis on complying with anti-corruption laws to “accurately reflect all transactions in Intel’s books and records.” (Intel, 2018).

## Fair Treatment

To treat each other fairly, Intel values open and honest communication, equal employment opportunities and diversity, anti-harassment, and safety. Meanwhile, Intel disapproves of human trafficking and forced labor as well as workplace violence.

Intel promises not to retaliate “against employees for asking questions or making good faith reports of possible violations of law, the Code, or other guidelines.” Intel values “the free flow of thoughts, ideas, questions, and concerns.” (Intel, 2018).

Intel promises not to discriminate or harass others based on “race, color, religion, sex, national origin, ancestry, age, physical/mental disability, medical condition, genetic information, military and veteran status, marital status, pregnancy, gender, gender expression, gender identity, sexual orientation, or any other characteristic protected by local law, regulation, or ordinance.” Intel promises to follow these principles during recruitment, hiring, training, promotion, compensation, benefits, transfer, and all other areas of employment and business. The code states, “We strongly disapprove of and do not tolerate harassment of employees by managers or co-workers.” (Intel, 2018).

Regarding child labor and forced labor, no one under 16 can work in any position and workers under 18 cannot perform hazardous work. These rules also apply to suppliers. (Intel, 2018).

Regarding workplace violence, Intel “will not tolerate threats of any kind, whether explicit or implicit, threatening behavior, stalking or acts of violence. We take all reports of threatening behavior or violence seriously, look into the matter, and take appropriate action.” In addition, Intel prohibits “harsh or inhumane treatment, including corporal punishment or the threat of corporal punishment. (Intel, 2018).

# Intel’s Guide to Privacy and Protection of Data

Intel’s Guide to Privacy and Protection of Data (2012) covers numerous topics relating to data, privacy, and existing legislation. This guide dives into Intel’s views on privacy and security and data breach notification, as well as actions the company has taken.

## Views on Privacy and Security

Intel realizes that consumer trust in companies is generally low. The guide proves this by sharing relevant survey results. For example, a 2009 study “found that 67% of those polled strongly agreed or agreed that consumers have lost all control over how personal information is collected and used by companies." (Intel, 2012).

The guide states that “Consumer trust is vital to the continued growth of e-commerce and the telecommunications sector.” Intel “believes the best way to ensure this trust is through the adoption of strong, technology-neutral legislation and international standards.” (Intel, 2012).

The guide explains many policies and acts and shares opinions on each. To demonstrate, it states the opinion that the Electronic Communications Privacy Act (ECPA) is outdated and “unable to appropriately address today’s technology.” The guide also shares information about Data Protection legislation in the European Union, U.S. Cybersecurity Legislation and U.S. Privacy Legislation. (Intel, 2012).

According to the guide, Intel “supports preemptive federal data breach legislation and believes that such legislation should be based on global norms.” Intel also supports the creation of a single, federal data breach notification standard. Intel acknowledges inconsistent data breach laws across U.S. states is an issue needed to be fixed by a federal data breach legislation. (Intel, 2012).

## Privacy and Security Implementations

Intel reinforces that they “work hard to create trust in the use of new technologies.” Intel invests significantly “in developing innovative security technologies which gain the benefit of operating in both hardware and software.” Intel “utilizes Privacy by Design and the Secure Development Lifecycle to develop products with both privacy and security in mind.” On the side of corporate citizenship, Intel works to “educate consumers about the importance of online data protection, and it is a proud founding sponsor of Data Privacy Day.” (Intel, 2012).

To minimize impact of data breaches, Intel has a privacy standards document which is based on the Fair Information Practices (FIP). The guide highlights three of the FIP principles they focus on regarding data breaches. First, Intel practices data minimization so “only the minimum amount of data necessary to accomplish a goal should be collected in the first place.” Second, Intel practices retention so data “should only be retained for as long as the purpose for which it was collected.” Finally, Intel practices proper transfer so “privacy and security requirements must be compiled with when transferring data to a third party.”

In a separate section titled Elements of Legislation, Intel has the full list of the FIP principles they follow. These include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability (Intel, 2012).

# Intel Corporate Privacy Rules

The Intel Corporate Privacy Rules (2015) document covers ethical practices for the protection, treatment, and sharing of data. In particular, it covers topics including collection and use of personal information, monitoring compliance to the rules, handling personal information requests and the complaint handling procedure.

## Collecting and Using Personal Information

Intel has 10 rules set for collection and usage of personal information. Each rule is closely related to the ten FIP principles.

1. Ensure personal information is collected and used in compliance with local law.
2. Ensure transparency by explaining to individuals how their personal information will be used.
3. Only collect and use information for purposes relevant to intel and the interests of the customer.
4. Ensure data quality by only retaining the relevant personal information needed for a purpose.
5. Take appropriate security measures by implementing appropriate technical and organizational measures to protect personal information.
6. Honor individuals’ rights by responding to all inquiries or requests made by individuals about their personal information.
7. Protect personal information transferred to third parties.
8. Safeguard the use of sensitive personal information, only using it if it is absolutely necessary and where the individual’s express consent has been obtained.
9. Never use personal information for direct marketing to a consumer unless the consumer has agreed to that use. Consumers can opt-out at any time.
10. Explain the logic used to make an automated decision about an individual if the individual requests it. (Intel, 2015).

## Audit Protocols

The document explains that Intel performs regular audits to check compliance to the corporate privacy rules. Audits cover “Intel’s information technology systems and databases, security policies, contractual provisions, training, privacy policies and guidelines.” Audits are performed annually or ad hoc if requested by the Global Privacy Officer, a data protection authority, or another “competent function.” (Intel, 2015).

## Complaint Handling Procedure

Any individual that believes that their information collected and used by Intel has not complied with the Intel Corporate Privacy rules is entitled to raise the matter with Intel’s Global Privacy Officer. The individual may also raise the matter with the relevant national data protection authority. Individuals can make a complaint by contacting the Intel Privacy Office online, with email, or in writing (Intel, 2015).

Intel promises to acknowledge receipt of a complaint within 5 working days of being received by the privacy office. Intel promises to respond to a complaint within 28 calendar days of receiving the complaint. If the complaint requires more than 28 days, Intel must provide an estimate not exceeding 6 months. (Intel, 2015).

# Brief Review of Meltdown and Spectre

In 2018, however, Intel started rolling downhill. In fact, Intel was not on Ethisphere’s 2018 list for the most ethical companies. This is likely because of Intel’s response to the Meltdown and Spectre leaks in its products.

Meltdown and Spectre were security flaws that affected most CPU chips manufactured by Intel. Meltdown was a vulnerability that allowed computer software to “melt” the security layer between it and the CPU’s memory, so it can access personal information and other information about the computer. Spectre breaks the security layer between applications, so in practice, an application would be able to steal cookies from your web browser (Meltdown and Spectre, n.d.).

Intel’s response to the flaw was meager. Intel did not initially tell computer emergency response teams (CERTs) and governments about the issue. This was supposedly because they would be unable to help fix the issue (Sharwood, 2018). Intel disclosed information about Meltdown and Spectre “only to companies who could assist Intel in enhancing the security of technology users.” (Sharwood, 2018). Intel only began to brief governments and the public about the issues once the news was leaked (Sharwood, 2018). Later, Intel sent letters sent to Congress that confirmed their plan to keep the CPU flaws secret to everyone else (Sharwood, 2018).

Intel has faced at least 32 lawsuits over the security flaws (Warren, 2018). Out of these, 30 were customer class action lawsuits filed to seek “monetary damages and equitable relief” for information leaked (Warren, 2018). The other 2 are security class action lawsuits which allege that “Intel and certain officers violated securities laws by making statements about Intel’s products and internal controls that were revealed to be false or misleading by the disclosure of the security vulnerabilities.” (Warren, 2018).

On a positive note, Intel was working behind the scenes to fix the issue and the security flaws were solved within a reasonable amount of time. In retrospect, however, Intel should have made the security flaws publicly known quickly so users and businesses could protect themselves.

# Conclusion

Excluding the 2018 security flaws and response, Intel’s ethics and privacy policies wonderfully reveal the company culture and the behavior to be expected. Workers at IBM should have no problems knowing how to treat employees ethically as well as protect and treat data in the perspective of privacy and safety. Reviewing each of these 3 documents, it is no question why Intel was one of the world’s top ethical companies for 2017.

# References

Intel. (2012). Data Protection and Security Policy. Retrieved from <https://blogs.intel.com/policy/files/2012/01/Intel_Priv_Sec_Guide.pdf>

Intel. (2018, January). Intel Code of Conduct. Retrieved from <https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/2018-intel-code-of-conduct.pdf>

Intel. (2015, December 15). Intel Corporate Privacy Rules Deed Poll. Retrieved from <https://www.intel.ca/content/www/ca/en/privacy/corporate-privacy-rules-deed-poll.html>

Kauflin, J. (2017, March 14). The World's Most Ethical Companies 2017. Retrieved from <https://www.forbes.com/sites/jeffkauflin/2017/03/14/the-worlds-most-ethical-companies-2017/#3f09408d7bc3>

Meltdown and Spectre. (n.d.). Retrieved from <https://meltdownattack.com/>

Sharwood, S. (2018, April 07). Intel didn't tell CERTS, govs, about Meltdown and Spectre because they couldn't help fix it. Retrieved from <https://www.theregister.co.uk/2018/02/23/meltdown_spectre_letters_to_congress/>

Warren, T. (2018, February 16). Intel facing 32 lawsuits over Meltdown and Spectre CPU security flaws. Retrieved from <https://www.theverge.com/2018/2/16/17020048/intel-spectre-meltdown-class-action-lawsuits>