ISSN: 2836-8495

Research Article

Journal of Current Trends in Computer Science Research

Exchanging or Thieving—A Foundational View of Software Ethics

Hamid A. Rafizadeh*

Emeritus Professor, Bluffton University

*Corresponding Author
Hamid A. Rafizadeh, Emeritus Professor, Bluffton University Adjunct Professor, University of Dayton, USA.

Submitted: 2024, Nov 02; **Accepted:** 2024, Dec 12; **Published:** 2024, Dec 19

Citation: Rafizadeh, H. A. (2024). Exchanging or Thieving—A Foundational View of Software Ethics. *J Curr Trends Comp Sci Res, 3*(6), 01-11.

Abstract

This article addresses the pressing issue of software thieving by using a software-update case study to examine the underlying ethical challenges in software production and usage. A proposed foundational framework highlights four critical factors: 1) the application of force, 2) the taking of resources, 3) knowledge processing, and 4) direction setting. This approach enables a comprehensive global analysis of the ethical dimensions in software development and use, contrasting voluntary exchanges with those compelled by thieving. Focusing on a case study of a large manufacturer, these foundational factors are applied to both individual and organizational behavior. The core challenge identified is the temptation for individuals and organizations to exploit the ease of force-driven resource acquisition rather than adhering to foundational ethical guidelines. Traditional reliance on published codes of ethics for moral reassurance is found to be inadequate, particularly within complex organizational structures where key decisions are pre-determined before employees are tasked with their execution. The foundational approach reveals the susceptibility of organizations to distorted and high-ignorance-content interpretations of law and ethics. This article outlines potential solutions to enhance ethical adherence, emphasizing the need for robust ethical guidelines that permeate all levels of decision-making within organizations.

Keywords: Software Ethics, Foundational View, Software Production, Software Use, Piracy

1. Introduction

In facing intense competition, software firms are increasingly turning to product families to efficiently support a product platform [1]. However, this strategy puts performance pressure on each family member, as the underperformance of one can adversely affect the entire family. Thus, the challenge lies in judiciously determining factors such as the number of products in the family, desired quality levels, time to market, and crucial success factors for improving a member's position, all while considering ethical implications and alignment with industry norms [2].

While software manufacturers design and deliver software with the intent of preventing or, at the very least, reducing exposure to external attacks [3], the effectiveness of a software's security architecture is compromised when the attacker is another software manufacturer. In that case, the methodology designed to address software vulnerabilities struggles to authenticate the actor, detect intrusion, revoke access, and audit, especially when confronted with the attacker disguised as a software update [4]. Regardless of the industry’s ethical framework, thievery represents a clear deviation from ethical standards, as it involves exploiting someone else’s software package for individual or organizational gain [5].

This article explores the study of ethical deviations through a concrete case study titled “John’s Case,” which focuses on a leading software manufacturer engaging in thieving through a software update mechanism.

2. The Case: Updating John’s Software

One morning, as John approached his computer, he noticed the need to log in, indicating recent updates. A dialog box revealed that Microsoft had updated Internet Explorer for better performance and virus resistance. However, when John clicked the Google button to access the university website for his mail, an unexpected screen posing as Microsoft Bing appeared. Despite verifying his selection, the Google button consistently redirected to Microsoft Bing. Even attempts to open Google from the start menu resulted in the same outcome—a frustrating Bing redirect. Perplexed, John turned to Firefox and searched for solutions online.

To his surprise, numerous articles addressed similar issues with titles like "How do I fix when I click on Chrome Bing opens" and "How to Remove Bing from Windows 10." Despite trying various suggested methods, none proved effective. One article suggested checking for Bing-related apps in the add-or-remove-programs section, but John found nothing named Bing, despite it being the only program opening when he clicked on Google.

After 45 minutes of fruitless attempts, exhausted and disheartened, John considered taking his computer to the university's computer center for assistance. In a moment of frustration, a new thought crossed his mind—there were no articles by Google or Microsoft addressing this problem. Their silence suggested either obliviousness to the issue or a deliberate choice to let it persist. Too fatigued to explore this thought further, John decided to contact the university's computer center and picked up the phone to schedule an appointment.

From Google's perspective, it is a well-established fact that they accelerate development, and improve learning by providing millions of code examples for software developers [6]. However, does this strategy inadvertently serve as a conduit for a competitor's developers to exploit Google customers, as seen in John's Case?

When assessing Microsoft's potential actions against Google, it is crucial to consider another facet of reality—the prevalent exposure of personal computers to piracy and viruses. The antivirus software is the conventional solution for viruses, and the industry offers various protective software to combat them. This response, however, fails to address a foundational problem in the knowledge flow within the software industry. The substitution of Google with Bing serves as an example of a virus-like software camouflaged as an update, representing a forced-on-consumer act of taking a competitor's resources through "authorized" computer break-ins. Existing antivirus defenses are ill-equipped to handle such self-authorized actions, particularly when orchestrated by a major software provider like Microsoft under the guise of a "software update."

Traditional protective measures operate under the assumption of intercepting and halting unauthorized actions. However, this approach becomes irrelevant when unauthorized actions, as seen in John's Case, are veiled within a major software manufacturer's self-authorized "software update." The software manufacturer knows the irrelevancy of the protective software and can assume that, in terms of knowledgebase and access to information, the user's capabilities are so minor compared to the manufacturer that they become inconsequential. This underpins the software industry's established stance that updates do not require user authorization, enabling providers, as in John's Case, to employ a forced-on-consumer marketing strategy, potentially influencing or dictating software usage.

In that setting, the challenge does not originate from unauthorized software copying but rather from an unethical act disguised as a legitimate software update. What might be typically labeled as piracy at the user level becomes an action akin to piracy orchestrated by a highly organized entity in the software industry, such as Microsoft Corporation.

3. A Foundational Analysis of the Situation

The traditional discourse on ethics and morality within software industry often centers on issues like the "loss of wealth" due to software theft and piracy [7-11]. However, this focus tends to overlook the broader ethical considerations related to the displacement of voluntary exchanges by forced exchanges.

A deeper examination of ethical behavior in the software industry requires an understanding of "foundational factors" to which, traditionally, the industry's ethics and morality discussions are not anchored. A compact view of foundational factors in any setting includes: 1) application of force, 2) allocation of resources, 3) access to knowledge, and 4) direction-setting [12]. These foundational factors depict individuals and organizations as force appliers, resource takers, knowledge processors, and direction setters.

Focusing on the second factor, resource taking, it is critical to recognize that the existence of every human and organization hinges on successfully taking resources from the Earth and other humans in order to satisfy one's daily needs in life. No human or organization would survive if taking of resources from the Earth and other humans ceases. The ethical considerations are intertwined with fundamental dependence on resource taking for existence.

Given that humans and organizations are inherently resource takers, societies have universally learned that voluntary rather than forced resource taking, particularly in the exchange of goods and services, is the most effective mode of human interaction. Within this framework, the individual or organization producing a good or service receives an additional increment of resources termed "profit" from the individual or organization using that good or service. The foundational basis of societal existence thus lies in "voluntary exchange-based resource taking." In contrast, the competing alternative is always "forced resource taking" in which there is no voluntary exchange. Ironically, while forced resource taking is the easiest method, the most difficult and most challenging approach, and at the same time most beneficial societally, involves resource taking through the voluntary exchange of goods and services [13].

Examining John's case from a foundational viewpoint reveals a lack of voluntary exchange. John did not choose to switch his browser from Google to Bing; he was compelled to undergo this change. Confronted by a powerful forcing agent, John found himself in a position that demanded accommodating and accepting the imposed alteration.

In his interaction with the forcing agent, John becomes acutely aware of the power wielded by invisible individuals and organizations. This power, viewed through a foundational lens, originates from four key sources: 1) control of application of force, 2) control of resource allocation, 3) control of access to knowledge, and 4) control of direction-setting [12]. All these factors are manifest and operational in John's case. The forcing agent dictates the direction away from Google and toward Bing, exercises control over access to knowledge—especially regarding how to reverse the switchover, manages the allocation of resources by determining which software can be accessed, and subtly deploys force to make this transaction enduring and seemingly inevitable. In essence, John navigates a landscape where these foundational sources of power shape and direct his personal experience.

In John's Case, is Microsoft the sole contender for the role of a forcing agent? Acknowledging that both individuals and organizations act as resource takers and force appliers, it is crucial to explore alternative possibilities. Dinita (2021) attributes the forced takeover of Google by Bing to malicious code infiltrating computers, stating, "Microsoft's search engine is often used by browser-hijackers." However, her argument falters when she conveys, "The good news is that the Bing redirects are rarely a phishing attempt or a full-fledged malware attack" [14]. This contradicts the fundamental understanding that humans, as resource takers and force appliers, are inherently driven by incentives to enhance their "resource position" and demonstrate "force superiority." Activities lacking incremental improvement in one's resource position are unsustainable, depleting the resource-taker's assets.

In support of the hypothesis that entities other than Microsoft could be forcing agents, Dinita adds, "The primary role of browser hijackers is to display intrusive online advertisements. They're also used to record your browser activity and gather personally identifiable information that is then sold to third parties." However, such forms of resource-taking can be executed more efficiently through Google, which boasts the highest market share, rather than through an invasive arrangement where a target like John would resist. Furthermore, as highlighted in Dinita's article and John's case, this intrusion occurs solely during Microsoft's software updates. Consequently, one can reasonably infer that Microsoft Corporation is the leading candidate as the forcing agent, while other browser hijackers have low to no plausibility in this role.

In an objective analysis open to all possibilities, one could entertain the notion that it is not Microsoft but Google orchestrating these intrusions, essentially attacking its own product to tarnish Microsoft's reputation. While this argument holds a low to very low plausibility, it paints Google as a potential forcing agent. However, even if Microsoft, Google, or both are considered as potential forcing agents, such a conclusion would underscore a significant dysfunctionality within another foundational factor of the software industry.

Throughout history, humans have organized their capabilities through the "manager-managed duality," where a small group, the manager, controls a larger number of individuals sharing their capabilities [15]. If this duality resorts to brute force to advance its resource-taking position through involuntary exchanges, the harm-based behavior renders it dysfunctional and ultimately destructive. In essence, organizing through a brute-force-driven mode can be likened to a "sick" organization that spreads its illness, seeing harming others as beneficial to its resource taking goals.

Examining John's Case through the lens of foundational factors reveals counterfeiting as another model for understanding Microsoft's behavior [16]. Counterfeiting can be either deceptive or nondeceptive [17]. Deceptive counterfeiting forces one to believe that a particular manufacturer's software is equivalent to another's, while nondeceptive counterfeiting typically involves a very cheap price. In John's Case, the new software is offered for "free," suggesting nondeceptive counterfeiting through a perfunctory logic that Microsoft's offer, being cost-free, is not misleading.

A more detailed perspective emerges when considering four distinct categories of counterfeits: counterfeit brands, pirated brands, imitation brands, and grey area products [18, 19]. In John's Case, the involvement is with the imitation brand, where the counterfeit software implicitly asserts to provide substance and performance akin to, or even superior to, the original software. This type of piracy is particularly insidious because "it is more challenging to define, identify, and label as illegal, as it is not necessarily a direct copy" [20]. Moreover, "consumers do not have much knowledge about various alternatives," a pivotal factor on which Microsoft capitalizes in John's Case [21].

4. The Role of Shared Capabilities

To understand competition from a foundational point of view, Rafizadeh (2018) employs the analogy of a water bottle to illustrate that every form of competition exists within a huge matrix of shared capabilities, involving millions of humans as capability sharers [22]. Extending this illustration, let us consider a single line of code and ask: How many individuals must share their capabilities to enable the creation of that line of code? Initially, we might focus on the individual who adeptly writes the code and inputs it into the computer. However, a closer examination reveals the indispensable role of the computer itself in completing the coding process.

One might argue that an individual does not necessarily require a computer to compose a single line of code and could achieve the task using pen and paper. But then, what about the pen or the paper? How many individuals must contribute their capabilities to provide the code writer with a pen or a sheet of paper?

I posit that the assertion that the shared capabilities of millions of humans are needed to produce a line of code remains valid regardless of the specific artifact involved. The demonstration of millions sharing their capabilities holds true whether we choose the chair on which the code writer sits, the room in which they work, or even the cup of coffee consumed during the code-writing process. In this instance, let us select the piece of paper and consider the capabilities of how many humans must be shared for the code writer to have that sheet of paper.

A sheet of paper is created from fibers extracted from wood through the pulping process, involving separating and cleaning fibers from wood chips produced by a woodchipper in a paper mill. A woodchipper, such as the "disc chipper," uses a steel disc with chopping blades or knives, consuming significant electricity. What capabilities must be shared for the woodchipper to operate and contribute to the paper-making process? Instead of directly answering, it is crucial to recognize that the woodchipper itself is constructed from metal, implicating the shared capabilities of countless individuals in the mining industry, metal processing, and manufacturing. From finding and mining ore to extracting the metal through mechanical and chemical processes, smelting, and electrical treatment, myriad capabilities are shared to produce the paper used for coding.

The foundational understanding of societal capability sharing extends beyond the code writer's connection to the paper mill. Once the paper mill creates the paper, a chain of interconnected capabilities is set in motion. The transportation of the paper necessitates a truck, which relies on the shared capabilities of numerous individuals in auto manufacturing. The truck's functionality is contingent on fuel, involving the shared capabilities of the entire oil industry, including refineries and gas stations. Furthermore, the truck cannot function without roads, involving the capabilities of road builders and constructors seamlessly integrated into the line of code. The paper mill's operation relies on electricity and natural gas, incorporating the capabilities of those in electric power plants, transmission and distribution lines, and natural gas pipelines into the code writer's paper.

Every participant identified in the process of sharing capabilities to bring the code writer's paper into existence relies on sustenance for their ability to contribute. Consequently, a portion of the capabilities of farmers and ranchers is woven into the fabric of the code writer's code. Beyond sustenance, the broader spectrum of capability-sharers requires essential services such as shelter, education, and healthcare. This leads to the integration of the capabilities of doctors, home builders, and teachers into the very essence of the code writer's line of code. In essence, the collaborative efforts of millions of individuals are needed for the development and sharing of capabilities, culminating in the code writer's ability to write a line of code.

This mode of thinking transcends writing a line of code and applies universally to product creation, services, and all aspects of human life, including the competitive landscape of the software industry. However, this foundational aspect of human existence, particularly the development and sharing of capabilities within the software industry, is often overlooked or rendered invisible. It should be apparent that the societal capability sharing system is indispensable for every individual and industry's existence. This intricate system sustains organizations across all industries, yet this crucial fact is most persistently overlooked by many.

The societal capability sharing system being a foundational prerequisite for existence of both individuals and organizations is not a new idea. Two centuries ago, Adam Smith observed that every aspect of an individual's clothing, tools and sustenance is the outcome of the collective labor of countless humans:

"Every part of his cloathing, utensils, and food has been produced by the joint labour of an infinite number of hands" [23].

While Smith employs the term "joint labor" instead of "capability sharing" and refers to "an infinite number of hands" rather than "millions of humans," the essence of the message remains unchanged.

The reality is that every individual and organization owes its existence to the capability sharing system. This must be a key consideration in any competitive strategy. Harming another organization reverberates through millions of individuals via the capability sharing system. Therefore, prioritizing the wellbeing of others is an irrevocable ethical imperative for the sustainable functioning of this system.

5. A Morality Problem—the Ignorance Content

In managing knowledge flow within the software industry, as well as any other field, a crucial and irreplaceable element is the "word," which serves as a carrier of knowledge in human interactions within organizational contexts, forming the foundation of any perspective, including that of John's Case. Thus, understanding the nature of "word" and its impact on ethical behavior is imperative.

Examining two models of the word—the suitcase model and the trousers model—reveals that universally, a word is a blend of knowledge (what humans know) and ignorance (what humans do not know). In the trousers model, the trousers symbolize the knowledge embedded in the word, while ignorance is personified as the entity wearing the trousers [24, 25]. The ignorance content of the trousers can be reduced by adding knowledge (other words) to the pockets. On the other hand, in the suitcase model, the suitcase's thin shell represents the smallest unit of knowledge encapsulated in a word. The empty space within the shell signifies the word's inherent ignorance, which is ever-present. The ignorance content of the suitcase can be reduced by introducing knowledge (other words) into the interior of the suitcase [26].

Consider the word "software" as an illustrative example. The suitcase and trousers of this word offer only a vague understanding of dealing with something digital. The word "Software" alone does not encompass knowledge of piracy, vulnerability to cyber attacks, data deficiencies, program failures, and numerous other complexities. All that knowledge has to be placed within the suitcase and in trousers' pockets to increase the word's knowledge content. The suitcase and trousers models of word point out that a word, by itself, is a high-ignorance-content artifact. Even with increased knowledge content, ignorance remains an inseparable feature of a word.

The concept of "ignorance content" holds profound significance, particularly within the software industry. Take, for instance, the widely acknowledged claim that the software industry suffers annual losses amounting to billions of dollars due to software piracy. Upon initial examination, we understand that fundamentally, every organization and individual functions as a "resource taker." However, both humans and organizations also serve as force appliers. Drawing upon millennia of collective experience, every individual and organization has come to the realization that acts of resource-taking must transpire within a framework of force-backed societal agreements, namely laws. These laws are upheld and enforced by society's concentrated brute force, manifested through institutions like courts, police, and armed forces. It is this force-backed arrangement that stabilizes resource-taking through voluntary exchanges, necessitating a keen awareness of "knowledge content" in these exchanges. The voluntary exchange-based resource-taking, therefore, operates as knowledge-driven endeavors within a matrix of force, acting as a societal stabilizer for the long-term existence of the society.

While a significant portion of resource takers adheres to the paradigm of knowledge-driven, voluntary exchange-based resource taking within the bounds of the societal force network, there exists a faction, comprising both individuals and organizations, that resorts to nonvoluntary force-driven resource taking. This form of resource taking focuses on exploiting the ignorance content, forming the foundation of issues like software piracy. Thus, the question arises: How does the software industry grapple with the complexities of software piracy?

To tackle nonvoluntary force-driven resource taking like software piracy, Moores and Chang (2006) suggest a four-word model focusing on recognition, judgment, intention, and behavior [27]. They argue that purchasing behavior is influenced by intention, which, in turn, is shaped by judgment. This approach aims to offer a nuanced strategy for addressing the ethical dimensions of piracy.

Without recognizing words as composites of knowledge and ignorance, we risk overlooking that terms like recognition, judgment, intention, and behavior do not offer a high-knowledge-content understanding of software piracy. However, this does not mean that the proposed four-word model has no value. Consider a scenario where a software company's management is under rigorous scrutiny by its board of directors and wants to showcase its proactive measures against software piracy. Despite its ignorance content, presenting this model to software company's board of directors can strategically support the claim of acting to reduce piracy levels. This form of "ignorance management" has its usefulness, even though it hides knowledge-based realities. Such approaches are prevalent in various organizational contexts, particularly in advertising, where high-ignorance-content communication is common. Politicians often employ it when interacting with constituents, and in varying degrees it exists in corporate communication dealings with shareholders, customers, and regulators.

It is imperative to recognize that words, whether embedded in a line of code or encapsulated in a four-word model of piracy ethics, play a pivotal role in mixing knowledge and ignorance to form knowledge-packet, often appearing as goods and services. Although Ostrom and Basurto (2011) may not be familiar with the suitcase and trousers models of words [28], and thus may not explicitly acknowledge the ignorance content of words, they astutely observe the inherent ambiguity in language, noting that "Rules are composed of mere words and … words are not always understood by everyone with the same meaning," highlighting the widespread challenge of Babbling equilibrium in human communication [29]. The term "babbling equilibrium" sheds light on how filling the suitcase or trousers of a word may vary among individuals.

In exploring the foundational basis of the four-word model of recognition, judgment, intention, and behavior, Moores and Chang refer to another four-component model rooted in moral psychology research [30-33]. This explanatory model comprises the following components [34]:

1. **Moral Sensitivity:** interpreting the situation as moral and exhibiting empathy for those involved.
2. **Moral Judgment:** determining which course of action is most justified.
3. **Moral Motivation:** deciding what one intends to do.
4. **Moral Character:** constructing and implementing a plan of action.

It is discernible that this new four-component model aims to augment the knowledge content of the preceding four-word model. Armed with the insights from the suitcase and trousers models of words, it becomes apparent that the new explanatory model deploys multiple words as empty-suitcase words. These encompass terms such as situation, empathy, course of action, justification, judgment, intention, character, plan, implementation, and prominently, the term "moral."

Within this new model, the word "moral" takes center stage, representing a high-ignorance-content feature across every component. Consequently, the new model becomes an assemblage of empty-suitcase words highlighting the term "moral." This raises the question of how such a model can enable the software industry to evaluate ethics and morality in actions and activities, particularly in contexts like piracy and responses to piracy. The subsequent section digs deeper into providing answers to this pressing question.

6. Ethics—A Deeper View

Ironically, ethics and morality stem from humanity's fundamental inclination to pursue individual desires without constraints, known as the "few-agree position." This inclination defines human existence, delineating individuals by their interests, preferences, perceptions, and opinions. Societal dynamics aim to reduce conflict among few-agree positions and foster cooperation by aligning diverse few-agree positions, resulting in collective agreements, or "many-agree positions," recognized as norms and standards, shaping anticipated behavior within society.

Human societies employ a two-tiered approach to assign significance to many-agree positions. In the first tier, certain positions are labeled "ethical/moral," while in the second tier, some evolve into "all-agree positions," universally enforced stances upheld by institutions like the police, armed forces, and courts. These enforced positions, or laws, essentially reflect force-backed many-agree positions [35]. It is crucial to note that all-agree positions emerge only through societal concentrated force combined with many-agree positions. Thus, what truly exists are force-backed or non-force-backed many-agree positions.

In society's collective fabric, myriad few-agree positions (ocean of FAPs) form the initial landscape, necessitating management, particularly in individual interactions. Many-agree positions serve as tools for navigating this landscape, aggregating to create the society's sea of many-agree positions (sea of MAPs). Managing diverse individuals within this framework proves challenging as individual FAPs often lead to confrontations. Each person tends to perceive their own FAPs as the sole appropriate behavior, resisting alignments dictated by MAPs. Lewis (2002) defines many-agree positions as a strategy for addressing the "coordination problem" inherent in confrontational FAPs [36], while Axelrod (1986) views them as norms regulating conflicts arising from aggregation of individual FAPs [38].

Given that only laws, as many-agree positions, are backed by societal concentrated brute force, how are other many-agree positions enforced without such backing? Axelrod (1986) outlines seven enforcement methods: metanorms, dominance, internalization, deterrence, social proof, group membership, and reputation [37]. Metanorm enforcement penalizes those who fail to penalize norm violators. Dominance involves one group imposing norms on another. Internalization conditions individuals, as in families, to self-enforce norms. Social proof sees individuals emulating observed behavior. The transition from group to societal enforcement requires significant force, resulting in the establishment of societal concentrated brute force via police, courts, and armed forces.

As a foundational factor, brute force maintains constant presence at human as force applier. In managing the sea of many-agree positions, it is important to note that all such positions, even if backed by force, function as mechanisms to shield everyone from direct exposure to “brute force” of humans as force appliers. This protective mechanism is notably exemplified in sharing of brute force, leading to formation of societal concentrated force (embodied by police, armed forces, and courts). This force is then applied through legal artifacts purportedly designed for the collective benefit.

The law, as a force-backed many-agree position, is the most conspicuous embodiment of this protective strategy, acting as a "force extension." Essentially, it extends the reach of societal concentrated force into individuals' daily lives, to shield them from direct exposure to concentrated brute force. This arrangement distances individuals from the immediate effects of brute force, creating an environment where, in effect, when every individual is aligned with force extensions, brute force seems virtually absent from human interactions [39].

This article's focus on John's Case and the software industry highlights the importance of addressing the management of "exposure to brute force" from the industry's perspective. Often overlooked is the fact that any attempt to seize a competitor's resources through the involuntary manipulation of consumers corresponds to breaches in the sea of many-agree positions, particularly the matrix of laws that channels brute force onto individuals. While Microsoft's promotion of Bing over Google may seem inconsequential, it exposes John to micro-level brute force. When multiplied by millions of others being subjected to such force-driven actions by multiple competitors, it sets the stage for a societal breakdown that could expose everyone to brute force. Historical instances, such as riots and revolutions, are rarely recognized as outcomes of the accumulation of numerous micro-level exposures to brute force, akin to John's Case.

An example of force management failure, falling short of riots and revolutions, is evident in the software industry, particularly when attributed to large companies. This failure stems from an inability to strike a balance between sharing capabilities to meet human needs and resource taking considerations. This failure invites the intervention of the societal force network to step in and overhaul force extensions, essentially reconfiguring the application of concentrated brute force. The goal of intervention is to create and provide a force-driven semblance of balance between shared capabilities and resource taking—a task the industry and its companies struggle to achieve autonomously.

The software industry's perception that using the societal concentrated brute force in the form of "force extensions" is a solution provider for its management deficiencies overlooks a crucial point: applying the societal concentrated brute force on individuals and organizations, however subtle it may seem, while potentially benefiting some companies in the short term and burdening others, invariably inflicts long-term harm on society. Exposure to brute force always equals harm. Ideally, the software industry, especially its major players, should engage in interactions in a harm-minimizing manner that restricts and prevents the application of brute force through laws developed by societal force managers—the politicians—to regulate the actions of companies. However, this vision often remains unrealized, primarily due to the industry's and its major companies' lack of awareness regarding the societal capability sharing system (SCSS) which in theory is designed to address the diverse needs of all. There exists a fundamental blindness to the fact that the industry and its major companies must assume the role of stewards for the health and well-being of the SCSS. This responsibility entails each participant watching out for others, despite their roles as competitive players in society's voluntary exchange-based resource-taking system within the broader societal matrix of brute and extended forces.

An illustration of the industry and its major companies' mismanagement of the Societal Capability Sharing System (SCSS) is evident in the lawsuits they file against each other, essentially employing societal concentrated brute force in industry matters. In a recent case, companies like Microsoft join government, the societal force manager, to accuse Google and Apple of stifling smaller competitors and engaging in profit-sharing agreements. As key industry players, it prompts the question: why do Google and Apple prioritize each other's interests over the wellbeing of other companies in the sector?

Consider the analogy at an individual level, where the denial of resource-taking opportunities within the extended force network may drive individuals to resort to brute force in the form of theft and robbery. Why do companies presume that a similar dynamic does not unfold at the organizational level? When organizations perceive threats to their resource-taking endeavors, they utilize "government" as their forcing agent. This coercion manifests itself in the form of lawsuits, akin to thieving and robbing but within the framework of legal proceedings. While the use of brute force disguised as law may seem to provide a more equitable distribution of resource-taking in the short term, it reflects industry's failure in managing the societal capability sharing system, resulting in long-term adverse effects.

Can managers, particularly those leading large corporations, recognize the foundational reality that every product or service, including all software, operates within a complex "network of forcing arrangements"? The industry's many-agree positions—whether explicit norms or hidden corporate strategies —have the potential to expose individuals to incremental doses of micro-level brute force, as seen in John's Case. Once subjected to such force, individuals or organizations may feel compelled to reciprocate, propelling their minds and organizational orientation into the realm of brute force as solution provider. Relying on brute force, akin to thievery, perpetuates the idea of resorting to force. Without integrating this perspective into decision-making, societal and industry dynamics may dysfunction. Escalating the force content of interactions disrupts voluntary behavior, prompting thoughts of retaliation and further eroding societal structure.

7. Emergence of Ethical Positions on Thieving

In John's Case, Microsoft's actions constitute a break-in, raising ethical questions. Ethical positions on break-ins vary, with some asserting that such actions are inherently harmful and wrong, while others suggest they might serve a purpose if no significant damage occurs. Thus, if John's computer sustains no serious harm, Microsoft's influence on his awareness of Bing could be viewed as valuable. Another ethical stance suggests that break-ins can only be justified in extreme situations, like life-threatening emergencies. Some argue that individuals breaking into computers are merely learning about system operations and programming complexities [40].

With Google dominating over 85% of the search market share and Bing holding just 7%, Microsoft's emulation of Google's search page features raises questions. Is it a learning process for Microsoft or a strategic move to enhance competitiveness? Additionally, Microsoft's tactic of incentivizing Bing usage with points redeemable as gift cards introduces another aspect, potentially exploiting human behavior as resource taker rather than emphasizing product value. This prompts scrutiny over whether Microsoft is genuinely learning and adapting to complex programming or simply capitalizing on behavioral tendencies to boost user engagement.

Views endorsing piracy also entertain the notion that software can attain consciousness and rebel against its usage. In this perspective, malware gains moral status as a protector against improper use. Mowbray (2021) suggests that malware design meeting consciousness-related criteria would trigger moral considerations and ethical protections [41]. Neely (2014) notes that the assignment of moral status to malware comes with "claims to self-preservation and autonomy" [42]. This raises the question: can Microsoft assert the right to self-preservation by displacing competing software?

The term "ethical" is a label that can be attached to any few-agree or many-agree position. When examining ethical views on software break-ins, one notable stance asserts that such actions align with the ethics of "all information should be free." [43]. However, this overlooks the understanding that everything humans make and use, including information, are knowledge-packets—a fusion of human knowledge with earthly materials. Whether it is a paragraph in a book, a loaf of bread, or a computer file, each represents human knowledge combined with earthly material, and none can be considered "free" in a society functioning on the premise of "resource taking." This reality is underscored by Baird et al.'s (1987) insight that "Crackers agree that computer-based information is a valuable resource.... Within the cracker subculture, information is used as a medium of exchange, it is the currency of the cracker" [44].

The argument for the positive aspects of "involuntary resource taking" can take various forms. Some suggest that communities benefit by learning from break-ins and preemptively addressing security issues that might otherwise go unnoticed. Another angle posits that "hackers break into systems to watch for instances of data abuse and to help keep 'Big Brother' at bay" [45]. Similarly, some argue that given no one is using a computer's full capacity, hackers should have entitlement to leverage idle systems. This perspective draws a parallel to the notion that numerous houses have unoccupied bedrooms, implying that anyone in need of a room should be able to use them. However, this logic for sharing idle assets, rooted in resource-taking, may exist as a few-agree position, and under specific circumstances, might even develop into a many-agree position. Nonetheless, whether a few-agree or a many-agree position, it will face intense competition from other few-agree and many-agree positions in society's ocean of few-agree positions (ocean of FAPs) and sea of many-agree positions (sea of MAPs).

8. Bring in Wealth

None of the various justifications for computer break-ins align with Microsoft's actions in John's Case. Instead, I will argue that Microsoft's conduct is motivated by considerations of "wealth." Wealth, often, is not understood as a key operational parameter for organizations that share human capabilities to produce goods and services to meet daily needs. Often overlooked is the fact that wealth, at both individual and organizational levels, is supported by three foundational functions [46].

1. Efficiency. As first foundational function, wealth serves as a measuring rod of assessing the "efficiency" with which individuals, organizations, or societies apply shared capabilities to fulfill human needs. Efficiency, depicted as an input-output relationship, necessitates that the resources entering the organization exceed those exiting. The difference is wealth, which keeps track of whether the individual, organization, or society is resource-efficient and capable of long-term survival and prosperity.

2. Value: In its second foundational function, wealth acts as a measuring rod of "perceived value" of goods and services to potential users. If no one values a good or service, no one will use any, rendering the organization unable to generate wealth. Failure to create value leads to unemployment for the worker and eventual demise of the organization.

3. Amplification of capabilities. The third foundational function of wealth is to serve as a measuring rod for the "amplification of capabilities." Wealth enables the holder to recruit personnel, acquire machinery, and organize capabilities to produce and distribute goods and services. Without wealth, these essential activities would be unattainable.

Understanding wealth's three functions reveals that in John's Case, Microsoft resorts to force because Bing fails to generate value compared to Google. When wealth cannot be generated within the extended force network, the only option is to venture into brute force. Microsoft easily leaks brute force into the consumer domain through updates of its other products, as seen in John's Case. Microsoft seeks to generate value for Bing by coercively compelling consumers to adopt it.

9. Discussion

Inherent to ethical conduct is the effective management of many-agree positions relevant to an organization's structure and operations. In analyzing John's Case, I have highlighted foundational factors at work in all organizations. Despite their pervasive presence in every organizational aspect, awareness of these factors remains low, potentially causing mismanagement of many-agree positions in the software industry, exemplified in John's case. Another significant contributing factor is the promotion of "oppositional positions" within software and other industries, deepening mismanagement of many-agree positions. To show how these oppositional positions eat away at the roots of every organization, including those in the software industry, I focus on oppositional positions advocated by Shoshana Zuboff (2020) [47].

In applying force, taking resources, accessing knowledge, and setting direction, every human function as a "choice maker" when it comes to making and using knowledge-packets, particularly those labeled as goods and services. That dynamic process gives rise to a comprehensive "choice making" database. In recent times, with enhanced technological capabilities, any organization can potentially leverage the choice making database in the pursuit of resource-taking and wealth making opportunities. This behavior is ingrained in humans and organizations as they act as resource takers and knowledge processors. The success of such behavior hinges on amplification of capabilities to enhance wealth generation through the efficient production of things that others value and need. Contrarily, Zuboff (2020) not only overlooks the foundational functions inherent in wealth but also mislabels the societal capability sharing system and the manager-managed duality within the force-based resource-taking system as "surveillance capitalism," while erroneously depicting the choice-making database as "free raw material." Zuboff's terminology fails to recognize the complexities of the manager-managed duality, the force-based resource-taking system, the societal capability sharing system, and the dynamics of the sea of MAPs and ocean of FAPs, where humans share capabilities to meet daily needs. This oversight constitutes a form of embedded "ignorance content" within her terminology.

What distinguishes Zuboff's terminology is its role in promoting an oppositional perspective on capability sharers within organizational contexts. What's particularly concerning is that these oppositional views consistently open the door for brute force to infiltrate the manager-managed duality, diverting attention from the intended focus on applying human capabilities to meet the daily needs of individuals within society's extended force network. Zuboff's oppositional stance does not search for a point of balance with other competing many-agree positions, instead aiming to establish itself as the sole surviving all-agree position, ultimately seeking victory over all other MAPs.

Let us follow the components of Zuboff's oppositional view, particularly as it pertains to software industry.

Zuboff (2020) opposes the notion of the choice-making database being utilized in machine intelligence to create prediction products traded in a new marketplace [48]. She views these projected knowledge-packets with suspicion, suggesting that surveillance capitalists profit immensely from these operations. However, her perspective lacks an understanding that a resource taker's standard behavior involves creating valuable knowledge-packets, offering them for sale, and profiting from successful sales.

Zuboff's reasoning overlooks the three foundational values of wealth: as a measure of organizational efficiency, a gauge of producing valued goods and services, and a metric for amplifying human capabilities to meet daily needs. Without recognition of these functions, Zuboff's oppositional stance becomes futile, fostering ignorance regarding the societal capability-sharing system and inviting brute force into human interactions.

Zuboff's position views humans as choice-makers whose personal experiences should not be packaged and sold for predictive purposes. Ironically, she advocates for the application of brute force to impose her perspective, proposing "extensive regulatory schemes" to curb surveillance capitalism. However, her lack of insight into human attributes like force applier, resource taker, knowledge processor and direction setter leads her to envision a force-driven social structure as the only framework for shared capabilities. Instead of advocating for a balanced approach rooted in a diverse sea of MAPs, Zuboff leans towards a force-amplified structure to bolster her position into an all-agree one.

Zuboff herself does not have the power to turn her many-agree position into a societal reality, but in John's Case, Microsoft does have the power to actualize its many-agree position by transferring value from Google to Bing. Both instances underscore the organizational and societal importance of managing the diverse sea of MAPs toward equilibrium, rather than using concentrated brute force to impose a particular viewpoint on all. Reflecting on Adam Smith's wisdom, he cautioned against managers imposing their favored many-agree positions as societal all-agree positions, highlighting the risk of using brute force to enforce personal viewpoints universally.

"The proposal of any new law or regulation of commerce which comes from this order, ought always to be listened to with great precaution, and ought never to be adopted till after having been long and carefully examined, not only with the most scrupulous, but with the most suspicious attention" [49].

Examining John's Case through Smeets' (2018) lens of transitory cyberweapons reveals a scenario where a cyberweapon assumes the form of a software update, posing challenges in identification and mitigation due to its rapidly changing nature. Smeets notes the advantageous offensive capabilities of such weapons, raising the likelihood of major software manufacturers engaging in dynamic cyber activities [50].

Axelrod and Iliev's (2014) strategic model sheds light on transitory cyberweapons, focusing on stealth and persistence [51]. Persistence is the likelihood that refraining from immediate use enables the cyberweapon to remain usable in subsequent periods, while stealth represents the probability that immediate utilization maintains its usability in the future. Regardless of these characteristics, piracy exploits architectural vulnerabilities. In theory, effective software design should aim to prevent or minimize such vulnerabilities [3, 4].

Bass et al. (2012) categorize strategies for developing attack-resistant software into four key areas: authenticating actors, detecting attacks, reacting to attacks, and recovering from attacks [52]. In John's Case, the Microsoft update possesses self-authentication and remains impervious to attack detection systems, challenging its identification until effects appear. The subsequent reaction and recovery depend on the individual's knowledgebase and the availability of a support structure. Baecker and Winter (2022) suggest countering cyberweapons by amplifying oppositional postures, advocating for individual self-control over technology usage and shareholder influence on companies [53]. However, their approach lacks a foundational sea of MAPs focus, relying on aligning behavior with specific positions that employ concentrated brute force, and overall, inadequate in protecting against cyberweapon use by large corporations.

10. Conclusion

Understanding foundational factors underscores the importance of avoiding competitive behavior rooted in "involuntary, force-driven" strategies aimed at seizing resources from others. The core challenge is whether individuals and organizations, acting as resource takers, can resist succumbing to the temptation of the ease inherent in the force-driven way of taking the resources of others. For Bing, competing with Google through voluntary exchanges is hard work, while replacing Google with Bing under the guise of a Microsoft software update presents a seemingly easier path.

Software engineers and manufacturing companies play a pivotal role in human existence and wellbeing by providing crucial software systems. Traditionally, the software industry relies on published codes of ethics for reassurance in ethical behavior. However, Gogoll et al. (2021) argue that this type of moral reassurance is deficient, especially within a company's multi-level decision-making structure, where key decisions regarding organizational behavior are already made before software engineers receive direction on assigned tasks [54].

External sources on ethical conduct offer limited assistance. In Hildebrandt's book, *Law for Computer Scientists and Other Folk* (2020), he posits that doing ethics can either mean engaging in the philosophical subdiscipline of ethics or acting ethically [55]. He overlooks the circularity of his statement, defining ethics in terms of ethics, rendering it a high-ignorance-content empty-suitcase word open to subjective interpretation. Furthermore, defining "law" becomes even more convoluted, as Hildebrandt relies on Uwe Wesel's assertion that "Trying to define law is like trying to hammer a pudding to the wall" [56].

My intent is not to undermine Hildebrandt's work but to underscore the software industry's susceptibility to distorted, high-ignorance-content interpretations of law and ethics, exemplified by Hildebrandt's perspective. This article aims to address such deficiencies by directly highlighting foundational factors of human existence, such as the ocean of few-agree positions, the sea of many-agree positions, the creation of privilege-label-driven many-agree positions using the terms ethics and morality, and the force-backed many-agree positions that transform into all-agree positions through societal concentrated brute force.

Armed with knowledge of these foundational factors, individuals can focus on managing and balancing the ocean of few-agree positions, the sea of many-agree positions, and societal concentrated brute force, enabling the fulfillment of daily human needs without exposure to brute force. Such an achievement is unattainable if ethics is perceived merely as being ethical, and law is seen as a pudding that can never be hammered to the wall.

References

1. Pohl, K., Böckle, G., & van der Linden, F. (2005). Software Product Line Engineering: Foundations, Principles, and Techniques. Berlin: Springer.
2. Alsawalqah, H. I., Kang, S., & Lee, J. (2014). A method to optimize the scope of a software product platform based on end-user features. *Journal of Systems and Software, 98*, 79-106.
3. Santos, J. C., Tarrit, K., Sejfia, A., Mirakhorli, M., & Galster, M. (2019). An empirical study of tactical vulnerabilities. *Journal of Systems and Software,* 149, 263-284.
4. Bass, L., Clements, P., & Kazman, R. (2012). *Software Architecture in Practice*, 3rd ed. Upper Saddle River, NJ: Addison-Wesley, Chap. 9.2.
5. Leventhal, L. M., Instone, K. E., & Chilson, D. W. (1992). Another view of computer science ethics: patterns of responses among computer scientists. *Journal of Systems and Software, 17*(1), 49-60.
6. Hora, A. (2021). Characterizing top ranked code examples in Google. *Journal of Systems and Software,* 178, 110971.
7. Brinkman, B., Gotterbarn, D., Miller, K., & Wolf, M. J. (2016). Making a positive impact: updating the ACM code of ethics. *Communications of the ACM, 59*(12), 7-13.
8. Marcu, D., Milici, D. L., & Danubianu, M. (2020). Software Engineering Ethics. *Postmodern Openings, 11*(4), 248-261.
9. Miocevic, D., & Kursan Milakovic, I. (2023). How ethical and political identifications drive adaptive behavior in the digital piracy context. *Business Ethics, the Environment & Responsibility, 32*(1), 256-273.
10. Moores, T. T., & Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *Mis Quarterly, 30*(1),167-180.
11. Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of business ethics,* 100, 405-417.
12. Rafizadeh, H. (2018). The Sucker Punch of Sharing. *Archway Publishing*. pp. 6–9.
13. Ibid, pp. 52–62.
14. Dinita, M. (2021). Why Is Bing My Default Search Engine? www.technipages.com/why-is-bing-my-default-search-engine. Accessed 7/10/2022.
15. Rafizadeh, H. (2018). The Sucker Punch of Sharing. Archway Publishing, p. 180.
16. de Matos, C. A., Ituassu, C. T., & Vargas Rossi, C. A. (2007). Consumer attitudes toward counterfeits: a review and extension. *Journal of consumer Marketing, 24*(1), 36-47.
17. Grossman, G. M., & Shapiro, C. (1988). Foreign counterfeiting of status goods. *The Quarterly Journal of Economics, 103*(1), 79-100.
18. Prendergast, G., Chuen, L. H., & Phau, I. (2002). Understanding consumer demand for nondeceptive pirated brands. *Marketing Intelligence and Planning, 20*(7), 405–416.
19. Lai, K. K. Y., & Zaichkowsky, J. L. (1999). Brand imitation: do the Chinese have different views?. *Asia pacific journal of management,* 16, 179-192.
20. Ibid, p. 180.
21. Ibid, p. 181.
22. Rafizadeh, H. (2018). *The Sucker Punch of Sharing.* Archway Publishing. pp 48-50.
23. Smith, A. (1982). Lectures on Jurisprudence. Liberty Classics, p. 340.
24. Austin, J. L. (1962). Sense and Sensibilia. London, UK: Oxford University Press, p. 70.
25. Hill, J. (2003). Meaninglessness: The Solutions of Nietzsche, Freud and Rorty [Book Review]. *The Australasian Catholic Record, 80*(3), 394-396, p. 395.
26. Rafizadeh, H. (2018). *The Sucker Punch of Sharing.* Archway Publishing. pp. 74–75.
27. Moores, T. T., & Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *Mis Quarterly, 30*(1), 167-180, p. 167.
28. Ostrom, E., & Basurto, X. (2011). Crafting analytical tools to study institutional change. *Journal of institutional economics, 7*(3), 317-343, p. 327.
29. Ostrom, E. (2005). *Understanding institutional diversity. Princeton university press*, pp. 176-179.
30. Narvaez, D., & Rest, J. R. (1995). The Four Components of Acting Morally. In Kurtines, W., Gewirtz, J. (Eds.), *Moral behavior and moral development: An introduction*, New York: McGraw-Hill, pp. 385-400.
31. Rest, J. R. (1983). Morality. In: Flavell, J. H., & Markman, E. M. (Eds.), Handbook of Child Psychology, Volume III (4th ed.). *New York: John Wiley & Sons,* pp. 556-629.
32. Rest, J. R., Bebeau, M., & Volker, J. (1986). An Overview of the Psychology of Morality. In: Rest, J. R. (Ed.), *Moral Development: Advances in Research and Theory*. New York: Praeger, pp. 1-27.
33. Rest, J. R., Thoma, S. J., & Bebeau, M. J. (1999). Postconventional moral thinking: A neo-Kohlbergian approach. *Psychology Press.*
34. Moores, T. T., & Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *Mis Quarterly,* 167-180, p. 168.
35. Rafizadeh, H. (2018). *The Sucker Punch of Sharing*. Archway Publishing, pp. 3-7.
36. Lewis, D. K. (2002). Convention: A Philosophical Study. Blackwell Publishers, Malden, MA, p. 5.
37. Axelrod, R. (1986). An evolutionary approach to norms.

American political science review, 80(4), 1095-1111.
38. Ibid, p. 1095.
39. Rafizadeh, H. (2018). *The Sucker Punch of Sharing*. Archway Publishing, p. 54.
40. Spafford, E. H. (1992). Are Computer Hacker Break-ins Ethical? *Journal of Systems and Software,* 17, 41-47.
41. Mowbray, M. (2021). Moral status for malware! The difficulty of defining advanced artificial intelligence. *Cambridge Quarterly of Healthcare Ethics,* 30(3), 517-528, p. 517.
42. Neely, E. L. (2014). Machines and the moral community. *Philosophy & Technology,* 27(1), 97–111, p. 106.
43. Spafford, E. H. (1992). Are Computer Hacker Break-ins Ethical? *Journal of Systems and Software*, 17, 41-47, p. 42.
44. Baird, B. J., Baird, L. L., Jr., & Ranauro, R. P. (1987). The moral cracker? *Computers & Society, 6*(6), 471-478, p. 472.
45. Spafford, E. H. (1992). Are Computer Hacker Break-ins Ethical? *Journal of Systems and Software*, 17, 41-47, p. 45.
46. Rafizadeh, H. (2018). *The Sucker Punch of Sharing.* Archway Publishing, pp. 64-68.
47. Zuboff, S. (2020). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: Public Affairs.
48. Ibid, p. 8.
49. Smith, A. (2003 [1776]). *The Wealth of Nations*. Bantam, p. 339.
50. Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies, 41*(1-2), 6-32.
51. Axelrod, R., & Iliev, R. (2014). Timing of Cyber Conflict. *Proceedings of the National Academy of Sciences, 111* (4), 1298–1303, p. 1299.
52. Bass, L., Clements, P., & Kazman, R. (2012). *Software Architecture in Practice,* 3rd ed. Upper Saddle River, NJ: Addison-Wesley, Chap. 9.
53. Baecker, R. M. (2022). Computing Ethics A Call to Action. *Communications of the ACM*, 65(3), 23-25.
54. Gogoll, J., Zuber, N., Kacianka, S., Greger, T., Pretschner, A., & Nida-Rümelin, J. (2021). Ethics in the software development process: from codes of conduct to ethical deliberation. *Philosophy & Technology, 34*(4), 1085-1108.
55. Hildebrandt, M. (2020). *Law for computer scientists and other folk.* Oxford University Press, p. 284.
56. Ibid, p. 17.