Smart Phones and Current Developments in Cyberwarfare: An Ethical and Anticipatory Ethical Analysis

Richard Wilson[1,2] and Noah Donnelly[2]
[1]Department of Philosophy, Towson University, Baltimore, Maryland, USA
[2]Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA

wilson@towson.edu
ndonnel1@students.towson.edu

Abstract: Smartphones in cyber warfare raise serious ethical concerns due to a number of factors including obscuring the line between civilian and military technology, how they expose non-combatants to harm, and how they lack clear international regulation. The central ethical issues related to the use of smart phones in cyber warfare include: (1) Civilian vs. Combatant Distinction. Smartphones are primarily civilian devices, yet they can be weaponized allowing civilians to engage in cyber-attacks. This development undermines the principle of distinguishing between combatants and non-combatants, a cornerstone of international humanitarian law. (2) Collateral Damage. Malware or cyber operations launched via smartphones can unintentionally spread to civilian networks, hospitals, or financial systems. Unlike traditional weapons, cyber tools are hard to contain, making unintended harm more likely. (3) Privacy Violations. Smartphones store vast amounts of personal data. Using them in cyber warfare risks mass surveillance, identity theft, and exploitation of private information, raising ethical questions about consent and proportionality. (4) Accountability and Attribution. Cyber-attacks via smartphones are difficult to trace. This creates ambiguity about responsibility, making it harder to hold aggressors accountable under international law. (5) Escalation of Risks. Since smartphones are ubiquitous, their use in cyber warfare lowers the threshold for causing a conflict. Everyday devices could become tools of state-sponsored attacks, increasing the risk of escalation into broader wars. (6) Lack of Regulation. Unlike conventional warfare, cyber warfare has no equivalent of the Geneva or Hague Conventions. The absence of agreed-upon rules leaves smartphone-based attacks in a legal and ethical gray zone. This analysis will identify the ethical and anticipated ethical issues with the use of Smart Phones in Cyberwarfare and the ethical and anticipated ethical issues with identifying smart phones as an important factor in cyber warfare.

Keywords: Cyber warfare, Smartphones, Stakeholders, Pegasus spyware, Civilian-Combatant distinction, Anticipatory ethics, Geolocation, Kinetic targeting

1. Introduction

Technology is moving towards integrating computing directly into human biology. We see this with new Brain Computer Interfaces (BCIs) like Neuralink. However, before addressing the ethics of a chip in the brain, we must first examine the ethics of the "supercomputer in the pocket" the smartphone. This paper argues that the smartphone ecosystem serves as a critical "ethical pilot program" for merging civilian life and military targeting. This pilot program is currently failing. The normalization of data vulnerability and the weaponization of consumer electronics have set a precedent. Civilian users are now treated as military sensors. By analyzing the current ethical failures of smartphones in cyberwarfare, we aim to establish a framework. This framework can prevent these same vulnerabilities from being hardwired into the human mind in the near future.

The development of Global Positioning Systems (GPS), high-resolution cameras, microphones, and constant internet connectivity have turned every smartphone into a possible node in military Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks (Singer & Brooking, 2018). The multi-use nature of these technologies creates a complicated ethical landscape. When a civilian uses a smartphone to film troop movements and uploads them to a social media platform, have they now become a combatant? When a state actor infects the smartphones of dissidents with professionally made spyware like Pegasus, does that constitute an act of war against another nation?

The importance and need for this analysis is shown by recent geopolitical events. In the war in Ukraine, smartphones have been used by civilians to report artillery targets, essentially crowdsourcing the “Kill Chain.” In the middle east, espionage software developed by private corporations have been used to assassinate journalists. In military bases, fitness tracking apps on smartphones have inadvertently revealed the locations of special forces outposts. These incidents demonstrate that smartphones are no longer just passive devices, they now allow their owners to become active participants in global conflicts. This analysis investigates the ethical and technical implications of this shift through four case studies: the Pegasus spyware developed by the NSO Group, Ukraine “Diia” app, the Strava Leaks, and the hacking of Jeff Bezos. This paper analyzes these incidents using the lens of Anticipatory Ethics and the ACM Code of Ethics. This paper argues that the designers of mobile

operating systems have failed to uphold the Sociotechnical Imperative by prioritizing convenience over security, jeopardizing the human user in a militarized world (Miller et al., 2011).

2. Technical Issues

To understand why the smartphone plays a central role in modern cyber warfare, one needs to examine the technical architecture within it which makes it both vulnerable and incredibly valuable to state actors for the purposes of cyber warfare. The smartphone is technically distinct from a laptop due to its intimacy, sensors, and connectivity.

The first significant vulnerability is **Sensor Fusion**. Modern smartphones are equipped with an array of sensors including accelerometers, gyroscopes, magnetometers, barometers, GPS receivers, and microphones. In a benign world, these allow for navigation, fitness tracking, and entertaining apps. In the context of warfare this is known as Sensor Fusion. A compromised smartphone can provide state actors with real-time, three dimensional, constantly updating images of the target's environment. Malware can activate the microphone to record classified conversations (SIGINT) or use the camera to gather visual intelligence (IMINT) unbeknownst to the user (Zuboff, 2019). The technical issue is these sensors are normally privileges at the hardware level, meaning that if a user disables "Location Servers" in the software, for security reasons, smartphone users do not have the kernel level permissions required to turn these off, meaning the baseband processor may still be communicating with cell towers, allowing for triangulation which reveals the location of the cell phone.

The second and most sophisticated form of smartphone warfare involves Zero-Click Exploits. Traditional malware requires user interaction, such as when a victim falls for bait in phishing. However, weapons like the NSO Group's *Pegasus* utilize vulnerabilities in the way smartphones process incoming data packets, such as an iMessage or a WhatsApp call, all of which happens before the user even receives a notification. This mode of attack targets the Baseband Processor, the chip that manages radio functions. Since the baseband runs a proprietary, closed-source real-time operating system (RTOS) with access to memory, exploiting this successfully would give the attacker the equivalent of System privileges on Windows (the most privileged account, not intended for human use). This technical reality renders traditional user and application-level defense mechanisms obsolete, there is no link to avoid clicking, thus no defense against the weapon.

A secondary technical threat is the physical supply chain and Hardware Implants. Smartphones manufactured in adversarial nations may contain hardware backdoors or firmware modifications designed to exfiltrate data to the opposing nations state intelligence services. This "interdiction" technique allows for the pre-positioning of cyber weapons within the civilian population of a rival nation. Since the global supply chain for smart phones is so complicated, components being sourced from dozens of countries, this in turn makes verifying the integrity of the hardware almost impossible. This creates a situation where the hardware acts as a hostile agent.

3. Ethical Issues

The weaponization of smartphones fundamentally changes the nature of warfare as defined in Just War Theory, more specifically, the principles of Jus in Bello (conduct in war). In Just War theory the main ethical framework for assessing these weapons is the conflict between military necessities and humanitarian protection.

The cornerstone of International Humanitarian Law (IHL), codified in the Geneva Conventions is known as the Principle of Distinction. Belligerents need to distinguish between combatants and non-combatants, which refers to valid and invalid targets respectively. Smartphones start to blur this line. If a civilian uses their smartphone to participate in a cyber-attack or to provide targeting data to a Telegram bot, they could potentially lose their protected status and become a legally legitimate target (Dawson & Innes, 2019). Unlike a soldier in uniform, a "digital combatant" may look exactly like a civilian. This creates an ethical crisis: if everyone has a smartphone, and every smartphone can be a weapon, is every civilian now a potential target? This logic leads to Indiscriminate Warfare, violating the core principles of humanitarian ethics as applied to warfare.

The Principle of Proportionality states that acts of warfare are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (International Committee of the Red Cross [ICRC], n.d.). Smartphone-based cyber weapons are incredibly difficult to contain. A "worm" designed to disable the phones of enemy officers that spreads by Bluetooth or Wi-Fi can infect the phones of hospital staff, aid workers, and children (Singer & Brooking, 2018). This "digital contagion" causes Collateral Damage not only to data, but to critical services that rely on mobile communications. Under Rights Ethics, this does not respect the right of security and safety afforded to civilians. Under ACM Principle 1.2 (Avoid Harm), the deployment of

uncontainable malware on civilian devices is an unethical renunciation of the developer's professional responsibility (Association for Computing Machinery, 2018).

Finally, the use of smartphones for mass surveillance violates Kantian Deontology. Kant argues that individuals must be treated as ends in themselves and not means. When a state transforms private devices of its citizens into a surveillance grid to root out insurgency or dissent, it treats its populus as a mere means and source of data. This destroys the concept of consent in regard to privacy (Nissenbaum, 2009). The user consented to carry a phone for communication, and not for the purpose of being a tracking beacon for a government. This is a breach of the "Digital Social Contract" and represents an immense ethical failure of both state and technology providers. This failure is worsened by "Normalization." The public has learned to accept total surveillance, seeing it as the "cost of doing business" in the digital age. This complacency creates a positive feedback loop. Civilians who accept vulnerability in peacetime become defenseless targets in wartime.

4. Case Studies

The theoretical risk of smartphone warfare has already materialized in many high-profile conflicts and worldwide espionage operations.

The most defining example of the weaponization of smartphones in the modern era is the "Pegasus" suite developed by the Israeli cyber-intelligence firm called the NSO group. Unlike regular malware which relies on "social engineering" (tricking the user into clicking on a malicious link), Pegasus introduced a new era of "Zero-Click" exploits. The technical sophistication of Pegasus represents a massive leap in offensive cyber warfare capabilities. In 2021, researchers at the Citizen Lab discovered the "FORCEDENTRY" exploit that targeted Apple's iMessage architecture. The exploit involved the sending of a malicious PDF file that was disguised as a GIF image to the intended victim's device. Inside the file was a stream of data encoded in the JBIG2 compression. The NSO Group engineers found that the JBIG2 vulnerability in Apple's "CoreGraphics" library was so extensive that they could build a primitive, emulated computer inside the memory of an iPhone's image processor. This let them execute malicious code by the phone trying to render a thumbnail which requires no interaction from the user. Once installed, Pegasus grants the attackers root access privileges. It can steal passwords, read encrypted messages on WhatsApp and Signal, track a user's location history, and activate the microphone and camera remotely. The unethical failures were revealed by the "Pegasus Project," when investigative journalists revealed that the software was not just used against terrorists, but against heads of state, human rights activists, and journalists. A prominent victim was named Hanan Elatr, who was the wife of murdered journalist Jamal Khashoggi. A forensic analysis showed that her Android phone was targeted by UAE officials using the NSO software months before her husband was murdered. This demonstrates how smartphones can be used by totalitarian regimes to extend their repression beyond their own borders.

Unknown to the world, the 2022 Crowdsourced Kill Chain of the "Diia" app and "GIS Arta" would spark what has be referred to as the first "Smartphone War." The Ukrainian government switched its pre-existing e-governance app, "Diaa" (Action), into a national defense weapon. They launched a feature known as "eVorog" (e-Enemy), allowing for any citizen with a smartphone to report the geolocation of Russian military assets. To verify authenticity, users had to sign in with their digital ID. This data was subsequently fed into "GIS Arta." GIS Arta collects civilian reports, drone feeds, and NATO intelligence to feed locations of targets to the nearest artillery battery, thus reducing the time from identifying a target to firing from 20 minutes to less than one minute. While it is an innovative strategy, this creates an enormous Anticipatory Ethical crisis related to determining the nonmilitary or military status of civilians. According to the Geneva Conventions, a civilian loses their protected status "for such time as they take a direct part in hostilities." By using smartphones to guide artillery fire, a Ukrainian grandmother can now technically become a combatant. This blurs the "Principle of Distinction" so far that it becomes nearly irrelevant within a modern battlefield. This also has the unintended consequence of inviting Russia to treat the entire cellular network as a military command-and-control system, which would justify broad kinetic attacks on cell towers and internet infrastructure, potentially going so far as to target of individuals holding smartphones in or around combat zones. This case study shows the transition of the smartphone from a device for communication to becoming a weapon in the "Kill Chain" in military operations (Claverie & du Cluzel, 2022). This creates a "Gray Zone" related to combatant status that current International Laws are not equipped to address.

In 2018, the fitness tracking application known as **Strava** released a "Global Heatmap" that visualized 13 trillion GPS data points collected from its users. While its intention was to show popular jogging routes, the map inadvertently unmasked secret military operations. Security analysists noticed in remote areas of Syria, Niger,

and Afghanistan, regions that should be dark, that there were bright data points with perfectly defined loops and lines. These were the jogging routes of U.S. and allied soldiers running the perimeter of what were supposed to be secret Forward Operating Bases (FOBs). This shows the dangers of "Passive Leakage" and "Pattern-of-life" analysis related to smart phones. The soldiers were not victims of being hacked, they signed a End User License Agreement (EULA) agreeing to the upload of their data. As a result, the collection of this data did not simply reveal where the bases were, but the operational tempo and supply routes of the forces inside these bases as well. By analyzing the timestamps of the runs, an adversary could gain an insight into patrol schedules and when shift changes occurred. This was a failure of the Sociotechnical Imperative by both the app developers and the commanding officers. Strava did not anticipate that when users of the tracking device set their participation to "public" by default they could compromise national security. In this case military commanders did not anticipate that a consumer device could be used as a tracking beacon.

The hacking of Amazon CEO Jeff Bezos in 2018 showed the world that the smartphone is a mode for the execution of high-level coercive diplomacy. According to a forensic analysis by FTI Consulting, Bezos' iPhone X was breached after receiving a WhatsApp video file sent from then personal account of the Saudi Crown Prince Mohammad bin Salman (Kirchgaessner, 2020). In a matter of hours of receiving the video, the device began sending out massive amounts of data, increasing from a daily average of 430KB to 4.6GB. This attack was not motivated by financial theft, but instead was aimed at gaining political leverage. At the time, *The Washington Post* (owned by Bezos) was aggressively reporting the murder of Jamal Khashoggi. The hack was meant to gather compromising material to blackmail Bezos, in order to have him give hush orders to his reporting staff. This incident single handedly destroyed the myth of "High-Value Target" immunity. At the time Bezos was the wealthiest man on earth, having access to the best cybersecurity resources, but was still vulnerable to a state sponsored "Zero-Day" exploit. It redefined smartphones as a weapon for Economic Warfare and political coercion.

5. Anticipatory Ethics

Applying the rules designed for assessing "Moral Responsibility for Computing Artifacts" by Miller et al. (2011) to the smartphone ecosystem can reveal significant ethical lapses in judgement.

The Sociotechnical Imperative states that "People who design... can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded" (Miller et al., 2011). Apple and Google designed iOS and Android for a sociotechnical system defined by "convenience" and "connectivity." By forging an ecosystem that prioritizes data collection for advertising and background connectivity for updates, they inadvertently built an architecture that is at its root vulnerable to surveillance. A responsible design for a "Warfare-Ready" world would include hardware kill-switches for microphones and cameras (Brey, 2012). Failing to include these features in their operating systems is a failure to anticipate the adversarial environment in which Apple and Google are embedding their your products.

Rule 1, The Foreseeability of Effect argues that "The people who design... are morally responsible for that artifact, and for the foreseeable effects of that artifact" (Miller et al., 2011). It was foreseeable that GPS tracking data from apps like Strava could be used for intelligence gathering. It was foreseeable that "Zero-Click" vulnerabilities in messaging apps like WhatsApp could be weaponized by state actors. The developers bear moral responsibility for prioritizing the release of new features at high speeds to attract consumers over security auditing to protect the customers who are buying their products. The failure to patch these vulnerabilities before they were weaponized and sold to entities like the NSO Group, demonstrates how developers neglected the foreseeable harm caused by their product. The "move fast and break things" philosophy of companies such as Facebook is indefensible when ethically scrutinized when the thing being broken is the product sold to customers whose physical safety of threatened.

Rule 2, What is called the Post-Deployment Mandate states that "Responsibility includes being answerable for the behaviors of the artifact... after deployment" (Miller et al., 2011). NSO Group likes to argue that they sell the software but are in no way responsible for its use. Anticipatory Ethics voids this defense. For a socially responsible creator of a cyber weapon this responsibility should also extends to post-deployment use. If the smart phone becomes a weapon and is used to target civilians, the creator of the smart phone shares in the user's culpability. Similarly, app stores have a post-deployment mandate to audit apps that serve as fronts for state surveillance, such as TikTok. The failure to monitor the ecosystem for weaponized applications is a clear neglect of the ethical responsibility one bears once the product has left the factory (Collingridge, 1980).

6. Recommendations

To begin, we must acknowledge the "Realist" critique. These security measures remain unimplemented because they contradict the current business models of surveillance capitalism and the strategic interests of state intelligence agencies. A hardware "kill switch" reduces the data collection capabilities advertisers rely on, and end-to-end compartmentalization hinders the ability of state actors to monitor threats. We contend that these recommendations, though commercially inconvenient, are ethically mandatory. As technology moves from "pocket" to "implant," the cost of maintaining this vulnerability gap will shift from financial loss to the loss of human cognitive autonomy.

The first recommendation is the implementation of a Hardware-Level “Kinetic Mode”. Manufacturers should implement a physical switch on devices, distinct from the software-based “Airplane Mode,” which can easily be bypassed by any attacker with deep systems knowledge. This switch would physically disconnect the circuit to the GPS, Microphone, and Baseband transmitter, only allowing locally stored maps and data features to function. This restores the Principle of Distinction by allowing a user to have a device that is verifiably “silent” and thus can not be targeted, avoiding collateral damage (Tavani, 2009). It moves the control of the device’s emissions from the software layer, which is hackable, to the hardware layer, which can provide a mechanical, unbreachable Killswitch.

The second recommendation is the adoption of a Zero-Trust Supply Chain. Defense contractors and Governments must be required to adopt a model where no component of a device is trusted by default. Smartphones used in sensitive contexts should be manufactured in secured, domestic facilities with firmware that can be audited comprehensively. This would uphold the ACM Principle 2.9 *Robust Security* and prevent the risk of foreign intelligence assets accessing domestic infrastructure. Without this, the hardware itself remains and must be treated as, a potential Trojan Horse.

The third recommendation is International Cyber-Arms Trade Regulation. The international community must treat “Cyber Weapons” such as Pegasus with the same scrutiny as kinetic weapons (ITAR). The sale of zero-click exploits to regimes that carry a poor human rights record must be banned from trade. Just War Theory and the goal of minimizing suffering align with such regulations. Limiting the spread of these weapons, could substantially reduce the likelihood of their use against non-combatants (Alabama Policy Institute, 2020).

The fourth recommendation is Operating Systems Compartmentalization. Mobile operating systems currently operate in the “Sandbox” model. We propose a shift to a strict Hypervisor-Based Virtualization model, similar to Qubes OS on desktops. In this architecture, the “Baseband” (radio), “Personal Space” (photos, chats, apps), and the “Work/Military Space” (sensitive data) would run in their own individual, completely isolated virtual machines (VMs). As smartphones currently stand, a zero click exploit in the iMessage parser (Personal Space) will increase its privileges to take over the entire kernel of a smart phone. In a virtualized environment, a malicious PDF exploiting the message parser would be trapped in the personal space with no access to the microphone, GPS, or other VMs. Furthermore, these virtual machines would not persist after a reboot, which would neutralize the lethality of weapons like Pegasus. This aligns with ACM Principle 2.9 *Designed for Robustly and Usably Secure Systems*. Assuming code will inevitably have bugs, this architecture minimizes the possible harm caused by these bugs, which fulfills the Foreseeability of Effect rule by designing for resilience rather than designing for perfection.

The fifth recommendation is Civic Digital defense Training. Since civilians are now participants in the “Kill Chain” (through apps like Diia), states have a moral obligation to provide Cognitive and Technical Defense Training. This would include public education campaigns related to a person’s own signal monitoring (e.g., why you shouldn’t use fitness trackers on base), spotting social engineering, and the risks of metadata. The “Human Factor” is and always will remain the weakest link. Even a perfectly secure architecture can be compromised if the user volunteers their location data to Strava. Training would reduce the “attack surface” by educating the population, thus making them harder to trick. If the state relies on the population for intelligence, it owes them the tools to survive the retaliation caused by their actions. Under Rights Ethics, not training civilians while encouraging them to use their phones for war is a dangerous form of negligence which allows them to be exposed to foreseeable harm.

The sixth and final recommendation is Legal Protections for Security Researchers. We recommend the establishment of internation at protection laws for security researchers who discover vulnerabilities in digital infrastructure. Currently, researchers who find flaws (like in the Strava leak) often operate in legal grey zones, and fear prosecution under laws like the Computer Fraud and Abuse Acts (CFAA). “White Hat” hackers are the

white blood cells of the internet, they find vulnerabilities before adversarial state actors can turn them into weapons. Punishing security researchers could create a ripple effect that leaves vulnerabilities unpatched. This analysis is supported by ACM Principle 1.5 *Respect the work required to produce new ideas* and 1.2 *Avoid Harm*. Encouraging a responsible disclosure of vulnerability will ensure design flaws are fixed, protecting the population as a whole. Any legal framework should view researchers as "Digital First Responders" as opposed to criminals.

7. Future Work

As stated in the introduction, the ethical failures observed in the smartphone era serve as a warning for the upcoming era of Brain-Computer Interfaces (BCIs). Future research should examine the ethical implications of Brain-Computer Interfaces (BCIs) and Augmented Reality (AR) contact lenses. If the smartphone is integrated directly into the human brain, such as a product like Neuralink, a "hack" could be considered a cognitive assault. A "Zero-Click" exploit in this new context could theoretically write data to the visual cortex, causing hallucinations or altering an individual's perception of reality. Additionally, future devices will track biometric data to infer a person's psychological states, by analyzing things like heart rate and cortisol levels. This enables "Pre-Crime" targeting. Pre-Crime targeting would target a soldier or civilian not because of where they were or what they did, but because of how they feel. This would represent the ultimate convergence of biology and technology in cyber warfare.

8. Conclusion

The smartphone has inherently changed the shape of the battlefield. It has democratized the gathering of intelligence, allowing civilians to act as sensors for military operations, but in effect they have also democratized targeting, turning every civilian into a potential beacon for a missile strike. The blurring of the distinction between a "Civilian Device" and a "Military Sensory" is a defining ethical crisis of modern cyber warfare related to the use of smart phones.

Through the analysis of Pegasus, Ukraine, and Strava, we conclude that the existing state of smartphones and how they are used in war are incompatible with the principles of International Humanitarian Law. Relying solely on software switches and closed-source basebands creates an environment of "Security Nihilism," where no user can be sure of their privacy and protected status. By applying Anticipatory Ethics, we identify that the burden lies with the architects of the technology being used. We need to abandon the "Consumer-Grade" mindset when designing devices that are currently being used in military environments. The Sociotechnical Imperative demands that we design devices which protect the user not just from potential spam, but from military targeting. Failing to do this ensures that in future wars, the existence of non-combatants with protected status, may no longer exist.

Ethics Declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI Tools Declaration: ChatGPT 5.1 for drafting and refinement. Human authors verified all content. Gemini 3.0 pro used for aiding in sourcing.

References

Alabama Policy Institute. (2020, November). *Understanding the Difference Between Positive and Negative Rights*. Alabama Policy Institute.

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

Brey, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. *NanoEthics*, 6(1), 1–13.

Claverie, B., & du Cluzel, F. (2022). Cognitive Warfare: The New Battlefield Exploiting Our Brains. *Polytechnique Insights*.

Collingridge, D. (1980). *The Social Control of Technology*. St. Martin's Press.

Dawson, A., & Innes, M. (2019). How Russia's Internet Research Agency Built its Disinformation Campaign. *The Political Quarterly*, 90(2), 245–256.

Federal Register. (2025). *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern* (89 FR 1636). U.S. Department of Justice.

Google Threat Intelligence Group. (2025). *Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis*. Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends

Harvard Kennedy School. (2025). *Ukraine's Digital Transformation: Innovation for Resilience*. Center for International Development. https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

International Committee of the Red Cross. (n.d.). *Proportionality*. How does law protect in war? - Online casebook. https://casebook.icrc.org/a_to_z/glossary/proportionality

Kirchgaessner, S. (2020, January 21). *Amazon boss Jeff Bezos's phone 'hacked by Saudi crown prince'*. The Guardian. https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince

Kirchgaessner, S. (2024, November 15). *NSO – not government clients – operates its spyware, legal documents reveal*. The Guardian. https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp

Knight First Amendment Institute. (2024, November). *Spyware Company NSO Group Faces Setbacks in Attempts to Avoid U.S. Lawsuits*. Columbia University. https://knightcolumbia.org/blog/spyware-company-nso-group-faces-setbacks-in-attempts-to-avoid-us-lawsuits

Miller, K.W., et al. (2011). Moral Responsibility for Computing Artifacts: 'The Rules'. *IT Professional*, 13(3), 57–59.

Miller, Maggie. (2025, May 6). *Israeli spyware giant NSO Group ordered to pay nearly $170M to WhatsApp for hacking accounts*. POLITICO.

Nestor, M.W. and Wilson, R.L. (2022). *Anticipatory ethics and the use of CRISPR in humans*. Springer.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Proctor, J. (2022, August 6). Dutch man Aydin Coban found guilty of extortion in Amanda Todd case. *CBC News*.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Eamon Dolan/Houghton Mifflin Harcourt.

SOC Prime. (2025, November 5). *CVE-2025-48593: Critical Zero-Click Vulnerability in Android Enables Remote Code Execution*. SOC Prime. https://socprime.com/blog/cve-2025-48593-vulnerability-in-android/

System and kernel security. (n.d.). *System and kernel security*. Android Open Source Project.

Tavani, H.T. (2009). *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Wiley.

What Is a Rendered Image on iPhone. (n.d.). *What Is a Rendered Image/Video on iPhone*.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.