Assignment 5.1: DMCA Cases

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

07/28/2025

Introduction

The rise of the Internet of Things (IoT) has transformed the digital landscape, connecting everything from home appliances to critical infrastructure systems. This technological evolution has opened new opportunities but has also expanded the attack surface for malicious actors. With billions of IoT devices now in operation globally, many of which lack strong security features, the risk of unauthorized access, data exfiltration, and system manipulation has grown substantially. These developments raise complex legal questions about access, modification, and software protection (Anderson & Rainie, 2021).

Legal precedents—particularly those involving end-user license agreements, software circumvention, and unauthorized access—are critical in determining how existing laws apply to modern cyber threats. The interpretation of these rulings shapes enforcement priorities, guides compliance strategies, and influences innovation. This paper examines three influential cases—*Davidson & Associates v. Jung*, *Philips North America v. Summit Imaging*, and *MDY Industries v. Blizzard Entertainment*—to extract key legal doctrines and apply them to contemporary cybersecurity and IoT-related challenges. In doing so, the paper offers a comprehensive assessment of current legal protections and recommends actionable policy improvements for organizations navigating these risks (Mireles & Hobaugh, 2024).

Case Analysis

Davidson & Associates v. Jung

In *Davidson & Associates v. Jung*, the defendants created a competing online service, Bnetd, that allowed users to play games like StarCraft and Diablo II without connecting to

Blizzard's proprietary Battle.net servers. To build Bnetd, the defendants reverse-engineered Blizzard's software, violating the End User License Agreement (EULA) and the Terms of Use (TOU) that governed access to Blizzard's games. Blizzard filed suit, claiming violations of the Digital Millennium Copyright Act (DMCA), specifically the anti-circumvention provisions, as well as breach of contract (Mireles & Hobaugh, 2024).

The court ruled in favor of Blizzard, holding that the reverse engineering violated both the EULA and the DMCA. The court emphasized that the defendants had agreed not to reverse-engineer the software when they accepted the license terms, and that their circumvention of the platform's access controls constituted an unlawful act. This case reinforced the legal strength of EULAs. It illustrated how contractual terms can be used to restrict reverse engineering, even when conducted for ostensibly non-malicious purposes such as enabling interoperability.

The key legal principle established in this case is that software owners can use licensing agreements to prohibit unauthorized access and reverse engineering. Even if such activities might otherwise be considered legal under fair use or certain DMCA exceptions, violating a contractual agreement can still result in liability. This ruling also demonstrated the courts' deference to private contractual terms over broader principles of innovation or consumer flexibility (Kerr & Solove, 2023).

Philips North America v. Summit Imaging

In this case, Philips alleged that Summit Imaging had circumvented access controls on Philips' diagnostic ultrasound machines. Summit, a third-party medical device servicing company, offered software tools that enabled healthcare providers to utilize Philips hardware

without requiring authorized access or licenses. Philips claimed that Summit's conduct violated the DMCA's anti-circumvention provisions and amounted to unauthorized access under common law (Mireles & Hobaugh, 2024).

The court agreed with Philips, stating that Summit's use of software to bypass security mechanisms—without Philips' consent—constituted a violation of federal law. Summit's actions were particularly significant because the equipment involved was medical, and unauthorized access posed not only a commercial risk but also potential public safety concerns (Perakslis & Stanley, 2016).

This case highlights a growing legal trend: manufacturers can and do utilize the DMCA to restrict third-party servicing and software-based repairs, particularly in sectors such as healthcare, where device integrity is crucial. The ruling also highlights how software embedded in physical devices is protected under copyright law, even when the user owns the hardware itself. The implication is that mere possession of a device does not grant the legal right to modify or access its software without the manufacturer's permission (Mireles & Hobaugh, 2024).

MDY Industries v. Blizzard Entertainment

The final case, *MDY Industries, Inc. v. Blizzard Entertainment, Inc.*, concerned a bot program called Glider that automated gameplay within Blizzard's World of Warcraft game. MDY Industries developed and sold Glider to players, allowing them to progress in the game without manual effort. Blizzard argued that Glider violated the EULA and TOU, and that it circumvented technological measures designed to detect and prevent bot use (Mireles & Hobaugh, 2024).

The Ninth Circuit Court ruled that although MDY did not directly infringe on Blizzard's copyright, it had violated the license agreement. More importantly, the court found that Glider's circumvention of anti-bot detection mechanisms constituted a violation of the DMCA. The court distinguished copyright infringement and license violations, clarifying that even in the absence of direct infringement, violating technological protections could incur liability under the DMCA (Kerr & Solove, 2023).

This case contributes a critical legal principle to cybersecurity law: circumvention of access controls can be actionable even when no actual copyright infringement occurs. In the context of software licensing, users can be held liable not only for their actions with a product but also for how they access and interact with it. This ruling reinforces the role of technological protection measures as enforceable digital boundaries, giving companies a powerful legal tool for shaping how their software is used (Mireles & Hobaugh, 2024).

Application to IoT and Cybersecurity

The rulings in these three cases provide a foundation for addressing modern cybersecurity threats in the IoT ecosystem. IoT devices often come embedded with proprietary software and are governed by terms of service or EULAs. The principles established in the aforementioned cases affirm the enforceability of these agreements and the DMCA's ability to deter unauthorized access or tampering (Mireles & Hobaugh, 2024).

In IoT environments, unauthorized access may occur when a user manipulates firmware, turns off security controls, or repurposes a device in a manner inconsistent with its intended use. These behaviors are parallel to the reverse engineering, circumvention, and automation scenarios addressed in the cases discussed. As such, the rulings support a legal

strategy that treats software-based device tampering as a violation of both contract and federal law (Kerr & Solove, 2023).

Nevertheless, challenges remain. Unlike traditional computing environments, many IoT systems lack clear user interfaces or access logs, making it harder to detect and prove violations. Additionally, IoT devices often operate autonomously, meaning unauthorized modifications can be made remotely without the user's knowledge. The lack of standardization in IoT security also complicates enforcement (Anderson & Rainie, 2021).

Another critical issue is the potential chilling effect on research and repair. Security researchers who attempt to identify vulnerabilities in IoT systems may find themselves in legal jeopardy due to anti-circumvention laws. This inhibits the discovery and disclosure of vulnerabilities that could protect end-users and infrastructure. Likewise, consumers and third-party repair services face legal risks when attempting to fix or enhance IoT devices—even when doing so is necessary for functionality, accessibility, or sustainability (Perakslis & Stanley, 2016).

While the cases validate the legal power of licensing and access controls, they do not adequately account for the complexities of good-faith security work or the repair rights of end-users. Current law leans heavily toward manufacturer control and away from openness, potentially hindering both innovation and safety. In IoT ecosystems, where the consequences of insecure devices can be dire, this imbalance warrants serious reconsideration (Mireles & Hobaugh, 2024).

Policy and Compliance Recommendations

To address the evolving risks in IoT security while aligning with the legal doctrines discussed, organizations should adopt a multifaceted approach to policy and compliance. First, companies must develop comprehensive EULAs that clearly define the scope of authorized use and explicitly prohibit reverse engineering, unauthorized firmware modification, and circumvention of security measures. These agreements should be easily accessible and written in language that is understandable to non-specialist users (Mireles & Hobaugh, 2024).

Second, organizations should implement technical safeguards such as cryptographic signing, secure boot processes, and encrypted firmware updates. These mechanisms serve as both deterrents and forensic tools, helping to detect unauthorized access and support legal enforcement when violations occur (Perakslis & Stanley, 2016).

Third, policy reform is needed to protect good-faith actors. Lawmakers should consider revising the DMCA to introduce safe harbor provisions for cybersecurity researchers and independent repair technicians who act in the public interest. These reforms should require responsible disclosure of vulnerabilities and promote collaborative efforts between researchers and manufacturers (Kerr & Solove, 2023).

Compliance programs must also be proactive. Security teams should perform regular risk assessments, monitor device behavior, and ensure that all stakeholders—from end-users to developers—understand the legal implications of their actions. Legal departments must stay updated on evolving interpretations of software law, particularly as applied to embedded systems and cloud-integrated IoT platforms (Mireles & Hobaugh, 2024).

Ultimately, a cultural shift toward transparency and accountability is necessary. Encouraging manufacturers to publish security standards, share update timelines, and engage with the cybersecurity community will foster trust and resilience. Regulation can play a role here by requiring minimum security baselines for IoT devices and enforcing reporting obligations for significant vulnerabilities or breaches (Anderson & Rainie, 2021).

Conclusion

The legal doctrines derived from *Davidson & Associates v. Jung*, *Philips North America v. Summit Imaging*, and *MDY Industries v. Blizzard Entertainment* offer a valuable framework for interpreting the rights and responsibilities of parties engaged with software-based technologies. These rulings affirm the enforceability of EULAs and technological access controls, providing manufacturers with powerful legal tools to protect their intellectual property (Mireles & Hobaugh, 2024).

However, the evolving nature of IoT ecosystems presents new challenges that these doctrines only partially address. While courts have consistently upheld the rights of software owners to limit access and modifications, the broader implications for cybersecurity, user rights, and ethical research must be considered. As devices become increasingly interconnected and embedded in critical infrastructure, the legal system must evolve to strike a balance between protection, innovation, and accountability (Kerr & Solove, 2023).

Moving forward, both private organizations and public institutions must collaborate to refine laws, implement innovative policies, and cultivate a secure and open technological landscape. Only through such a coordinated approach can the benefits of IoT be fully realized without compromising the integrity of the digital ecosystem (Anderson & Rainie, 2021).

References

Anderson, J., & Rainie, L. (2021). The Internet of Things connectivity binge: What are the implications? *Pew Research Center*. https://www.pewresearch.org/internet/2021/06/30/the-internet-of-things-connectivity-binge-what-are-the-implications/

Kerr, O. S., & Solove, D. J. (2023). *Cybersecurity law: Technology and actors* (Ch. 2). West Academic Publishing.

Mireles, M. S., & Hobaugh, J. L. (2024). *Principles of cybersecurity law* (2nd ed.). West Academic.

Perakslis, E., & Stanley, M. (2016). A cybersecurity primer for connected medical devices. *Brookings Institution*. https://www.brookings.edu/articles/a-cybersecurity-primer-for-connected-medical-devices/