Jasvinder Mannn

Western University, London, ON, Canada

Alissa Centivany

Western University, London, ON, Canada

Steering the Narrative: An Analysis of how Cybersecurity Rhetoric is used to Hinder the Right to Repair

Abstract

The intersection of consumer rights and corporate control is exemplified in the battle over automotive repairability, where claims of cybersecurity risks challenge the Right to Repair movement. This study critically examines challenges to Massachusetts' Data Access Law, which sought to expand independent access to vehicle telematics data for purposes of diagnosis, maintenance, and repair. Through critical discourse analysis, the findings expose rhetorical strategies that prioritize corporate interests under the guise of safety. This research emphasizes the need for policy interventions that prioritize transparency and innovation and recognize that robust security and equitable access to repair can coexist.

Introduction

From cars and personal electronics, to tractors and military equipment, to CPAP machines and hospital ventilators, to the soft-serve machine at McDonald's, fixing things after they break is increasingly difficult if not impossible (Blanco, 2023; Ekman, 2019; Gault, 2023; Koebler, 2018, 2020; Stanton, 2022; Waldman & Mulvany 2020). In the interest of economic affordability and environmental sustainability, lawmakers in the United States, Canada, the European Union and elsewhere are exploring "Right to Repair" as a way to temper repair restrictions and extend the useful life of the things we own (Bill C-244, 2024; “Is There A Right to Repair,” 2023; Moore, 2018; Perzanowski, 2020; Pihlajarinne, 2020). Meanwhile, opponents of these measures are busily preserving repair roadblocks through design choices, business strategies, lobbying, and raising various alarms in testimony before lawmakers (LaForest, 2020; Mirr, 2019; Montello, 2020). A few arguments are routinely put forth by Right to Repair opponents. This research explores one in particular: security.

A point frequently raised by opponents of the Right to Repair is that reducing or removing obstacles for consumers and independent repair technicians to fix broken equipment will raise security concerns (Forno, 2021; Roberts, 2023). Reparability, according to opponents, inherently poses risks unless repairs are conducted by "authorized" technicians. But are these claims genuinely valid, or do they serve as rhetorical fearmongering? In Canada, parliamentary testimony by members of industry, academia, and advocacy groups makes clear the central, contentious role that security concerns play in the Right to Repair (Canada, Parliament, House of Commons, Standing Committee on Industry and Technology, 2023). In her testimony before the Canadian House of Commons and Senate, Centivany testified that industry and lobbyist arguments that accessible repair undermines security are anti-consumer, anti-innovation,

unsupported by evidence, and rebutted by the industry's own pattern of embedded insecure features and systems in their vehicles (Centivany, 2023a,b; Centivany, 2024a).

The significance of the automotive sector in this discourse is vital and multifaceted. Car repair costs have escalated significantly, with a nearly 20% increase from 2022 to 2023, as reported by the consumer price index (Iacurci, 2023). This cost factor is compounded by the increased incorporation of smart technologies in both EVs and gasoline vehicles, which include data tracking capabilities, amongst other ethically dubious advances (Iacurci, 2023).

The automotive industry has emerged as a significant area of concern regarding data security and privacy. A recent report revealed that, of the 25 brands evaluated, 84% share consumers' personal data with entities such as service providers, data brokers, and other businesses, raising critical security concerns (Caltrider et al., 2023). Perhaps even more concerning, 56% of these companies revealed that they may share such data with government or law enforcement agencies upon request, often without requiring a judicial warrant (Caltrider et al., 2023). This lax approach to data sharing stands in stark contrast to the heightened security claims auto manufacturers invoke when opposing repair shops' access to vehicle data. Such discrepancies raise crucial questions about the industry's motivations and priorities. This paper will critically analyze a key case where these tensions converge, shedding light on the broader implications for security, repair, and regulatory practices.

Automotive Data Access for Repair

In the legal landscape of automotive repair, Massachusetts has been at the forefront of protecting consumer rights. The state enacted its initial Automotive Right to Repair statute in 2013, a seminal piece of legislation that mandated manufacturers to furnish independent repair facilities with the same diagnostic and repair information available to franchised dealerships (Mass. Gen Laws Chapter 93K, 2013; Stone, 2023). The law, brought forward as a referendum, sent a loud message to the automotive sector that the public demands a choice in selecting repair service providers and they were not content relying solely on authorized dealers. This statute did not address telematic data, a gap that became increasingly problematic as vehicles adopted more sophisticated computational systems (Stone, 2023).

In response to these evolving challenges, Massachusetts voters approved a ballot measure in 2020, commonly referred to as the Data Access Law (Banner, 2023 ;Stone, 2023). This law extended the Right to Repair framework to include telematic data, thereby compelling manufacturers to grant both vehicle owners and independent repair shops access to this crucial information. While the statute ostensibly aims to democratize the automotive repair market, it also implicates broader public policy concerns, including environmental sustainability. The law's environmental ramifications are particularly salient given the carbon-intensive nature of vehicle manufacturing, especially in the context of electric vehicles.

Nevertheless, the Data Access Law has been met with considerable legal resistance. The Alliance for Automotive Innovation (AAI), representing various automakers, has initiated litigation to prevent the enforcement of the statute (LaForest, 2023). The crux of the industry's argument hinges on the purported cybersecurity risks and potential conflicts with federal safety regulations that could arise from making telematic data more accessible. This line of reasoning, however, has been critiqued for relying on the concept of "security by obscurity," a cybersecurity approach that is increasingly viewed as outdated and ineffective by experts in the field. In 2021,

Attorney General of Massachusetts Maura Healy (now Governor) said that she wouldn't enforce the law until it was decided in federal court (Banner, 2023). Attorney General Adrea Joy Campell said she would enforce the law after a Temporary Restraining Order (TRO) by the AAI was denied (Banner, 2023). This law was set to be enforced beginning June 1st, 2023.

However, soon after, on June 13th, 2023, a letter from the National Highway Traffic Safety Administration (NHTSA) signed off by Kerry E. Koloziej (Assistant Chief Counsel for Litigation and Enforcement at NHTSA) was sent to the counsel vehicle manufacturers regarding the Massachusetts Data Access Law, to not follow it as it did not comply with the federal Safety Act. The recipients of this letter included legal representatives (or counsel) from 22 car manufacturers that operated in the state. Analysis of this letter will be a primary focus of our study, as it provides insights into how rhetoric around security is employed to shift perceptions, particularly as it relates to repair.

The NHTSA's stance, emblematic of a top-down approach, has been met with resistance from influential political figures, particularly U.S. Senators from Massachusetts, Elizabeth Warren and Ed Markey (Warren & Markey, 2023). On June 15th, 2023, the senators issued a joint response, underscoring the undemocratic nature of disregarding the popular will. The letter discusses Massachusetts Question 1, the "Right to Repair Law" Vehicle Data Access Requirement Initiative (2020), which was endorsed by an overwhelming majority of approximately 74.97% of voters (Ballotpedia, 2020).

The Senators' letter, however, goes beyond mere opposition. It highlights an inconsistency between the NHTSA's position and President Biden's Executive Order on Promoting Competition in the American Economy (Exec. Order No. 14036, 2021). The order explicitly condemns excessive concentration of industry and market power abuses, particularly in various sectors, including repair markets. This condemnation aligns with broader economic policies aimed at fostering competition and preventing monopolistic practices. The Senators concluded their letter by posing a series of critical questions, seeking clarity on the timing, validation, consultations, and alternative approaches considered by the NHTSA. These inquiries, which remain publicly unanswered, highlight the divisive nature of the Right to Repair issue, revealing a division within different governmental branches. The lack of transparency and the apparent contradiction between executive actions and legislative intent underscore the complexity of the issue.

On August 23rd, 2023, in a recent and significant policy shift, the NHTSA withdrew its opposition to the Massachusetts' Data Access Law (Lowery, 2023; Marshall 2023). This is noteworthy for many reasons, as it demonstrates the regulatory stances in the face of advancements in technology as well as public and political pressures. This reversal of position presents a more nuanced understanding in the design of products and that cybersecurity and repair do not need to be mutually exclusive features. The NHTSA said that auto manufacturers could comply with the Data Access Law by using short-range wireless protocols like Bluetooth to allow vehicle owners and repair shops authorized by the owner to access the necessary data (as defined in the law) of that vehicle (Lowery, 2023; Marshall 2023).

Methodology

The NHTSA letter is a crucial document for analyzing the cultural and political dynamics of the Right to Repair movement. As a pioneer in this area, Massachusetts set a national precedent with

its 2013 automotive Right to Repair law (Grinvald & Ofur, 2021), later expanded in 2020 to include telematics data. By opposing this law, the NHTSA not only challenges the will of Massachusetts voters but also undermines the foundational progress of the movement. This letter was selected for data analysis as it encapsulates the key tensions and rhetoric shaping repair rights at both state and national levels.

To analyze these dynamics, this study employs critical discourse analysis (CDA) as its methodological framework. CDA offers a powerful tool to examine how the language in the NHTSA letter reflects and reinforces power structures, particularly through its framing of safety, authority, and compliance (Fairclough, 2013). Special attention will be given to how the letter invokes cybersecurity and data protection to justify limiting access to telematics systems. By scrutinizing rhetorical strategies, linguistic choices, and underlying assumptions, this analysis will reveal how these arguments are constructed to portray repair access as inherently risky. CDA will also explore how these narratives implicitly prioritize corporate control and monopolistic practices under the guise of safeguarding public safety and cybersecurity. Through this approach, the study seeks to uncover the broader implications of this discourse, particularly how language is used to marginalize independent repair and obscure alternative frameworks for secure and equitable access.

Critical Discourse Analysis: NHTSA Letter

This letter, a response to the Data Access Law in Massachusetts which the NHTSA says poses safety concerns, calls on manufacturers to follow their obligations under the National Traffic and Motor Vehicle Safety Act, such as preventing serious injuries by defects before they occur. The letter's employment of legal and technical language serves multiple functions. By referencing specific laws, court cases, and technical terms related to vehicle telematics, the NHTSA establishes itself as an authoritative and legitimate arbiter of safety and law. This specialized language not only positions the agency as an expert but also creates barriers to understanding for those without specialized knowledge, potentially excluding some from the discourse.

Furthermore, the authority here can be seen as a power play against a state government. It presumes the NHTSA has jurisdictional authority over a state law that was introduced as a referendum and was carried by an overwhelming majority of voters. The formality of the letter presented in its language and structure, reflects, at best, a lack of sensitivity to the issues at stake, and, at worst, could be interpreted as an attempt to overpower through officiousness. This tactic reveals how language can be used to construct and reinforce power relations. The appeal to legal obligations within the letter serves to delegitimize the Massachusetts law, positioning it as an aberration that must be corrected. By framing compliance with the Data Access Law as a conflict with federal law, the letter subtly coerces manufacturers into alignment with the NHTSA's position. This appeal to higher authority reveals the complex interplay of legal and rhetorical strategies, reflecting the contested nature of the issue.

The letter's implicit endorsement of security through obscurity, a discredited approach that relies on secrecy as a means of protection, further aligns with corporate interests. As highlighted by cybersecurity professional and Right to Repair advocate Paul Roberts, this approach is flawed and overlooks the inherent vulnerabilities of closed systems (Roberts, 2023). By endorsing this approach, the letter reinforces power imbalances between manufacturers and consumers, reflecting the broader tensions between openness and control in the technological domain.

The letter's repeated emphasis on safety concerns constructs a narrative where the Right to Repair is inherently dangerous. Phrases such as "significant safety concerns," "unreasonable risk to motor vehicle safety," and "serious safety risks" are strategically employed to associate the Right to Repair with foreseeable crashes, injuries, and deaths. By foregrounding safety, the letter appeals to a universal value that is difficult to contest, effectively silencing other considerations such as consumer rights, competition, and sustainability. This framing serves to reinforce existing power dynamics, aligning with corporate interests and privileging the NHTSA's position over other stakeholders.

The construction of a false dichotomy between safety and the Right to Repair further illustrates the letter's rhetorical sophistication. By suggesting that open remote access to vehicle telematics necessarily entails risks to safety-critical functions such as steering, acceleration, and braking, the letter creates a binary opposition that overlooks the possibility of designing secure and accessible systems. Terms such as "open access allows for manipulation" and "malicious actor here or abroad" evoke images of uncontrolled and nefarious intrusion, reinforcing this dichotomy and marginalizing alternative perspectives. This framing is challenged by independent experts, such as those cited in the Stanford Cyberlaw Blog's article, who argue that restricting access is not necessary for cybersecurity (Forno, 2021). The construction of this dichotomy reveals the underlying ideologies and assumptions that shape the discourse, reflecting broader struggles over control, rights, and justice in the technological landscape.

Ambiguities and contradictions within the letter further add to its complexity. For example, the letter acknowledges the importance of consumer choice in vehicle servicing and repair but then argues that this choice must not pose a risk to safety. It also recognizes the benefits of telematics data for emergency response and safety oversight but then warns against the risks of open access. These contradictions reveal the underlying tensions and competing interests at play in the discourse, providing insights into the broader socio-political dynamics. The letter's conclusion, with a call to action expecting manufacturers to comply with federal safety obligations, serves to reinforce the NHTSA's authority and align manufacturers with the agency's position. This call also implicitly warns against non-compliance, reflecting the coercive undertones of the letter and the broader power relations at play.

Discussion

The NHTSA letter uses specialized language to assert authority, framing the Right to Repair as a risk to safety while marginalizing alternative perspectives. This rhetoric prioritizes corporate interests, highlighting the divisive nature of the debate and exposing tensions between governmental branches and public and corporate priorities. The lack of transparency and contradictions in the letter, such as acknowledging consumer choice while limiting it through safety concerns, underscoring the complexity of the issue. Addressing these gaps requires a more inclusive and transparent policymaking approach that balances safety, competition, and consumer rights.

Additionally, regulatory capture may influence the NHTSA’s actions in this case. This economic theory suggests that regulatory agencies, intended to serve the public interest, can become aligned with the industries they oversee (Dal Bó, 2006; Li, 2023). This often occurs as regulators are drawn from industry due to their specialized knowledge and may later return to private sector roles, a phenomenon known as the “revolving door” (Zheng, 2014). For example, Kerry E. Kolodziej, who signed the NHTSA letter as Assistant Chief Counsel for Litigation and

Enforcement, previously worked at Mayer Brown LLP, which now represents the Alliance for Automotive Innovation (Alliance for Automotive Innovation v. Healey, 2020; DRI Faculty List, 2017; LAW360, n.d.; Kerry Kolodziej, n.d.). Similarly, a former NHTSA Chief Counsel later joined Mayer Brown as a partner, exemplifying the movement of personnel between regulatory and industry positions (DRI Faculty List, 2017). While such transitions do not inherently indicate corruption, they raise concerns about cognitive biases or a worldview favoring corporate interests.

The automotive industry's use of cybersecurity as a barrier to repair access reflects "security theater" these are practices that project safety without substantive improvements (Schneier, 2008). This tactic shields monopolistic practices while failing to address inherent data vulnerabilities, disproportionately affecting marginalized consumers who lack alternatives. Security concerns persist regardless of repair access, as manufacturers' internal data handling can also lead to misuse. True autonomy lies in empowering product owners with data control.

Security threats to the consumer do not just vanish if the device is sent to the manufacturer, there are people that work there that may access data that is not required and can misuse it. The autonomy of who can access the data should reside with the owner of the product. Our recommendation from a technical perspective is to implement security safeguards that are similar to Samsung's "Maintenance mode," which allow phone repair without access to personal data (Samsung, n.d.). In this case car owners can control and block or control certain points of data that need to be used during repair. Also similar to the software that can track what was seen on phones or laptops, having a tracking receipt of what was accessed and used during the repair process of cars allows the owner to audit if things were done correctly or have a third party check the tracking receipt if further technical knowledge of the process is required.

Conclusion

The NHTSA letter exemplifies how language and policy can prioritize corporate control under the guise of safety and security. Addressing these challenges requires balancing security with transparency and equity, ensuring consumers retain autonomy over their devices without compromising safety. Incorporating technical safeguards, such as controlled data access and audit mechanisms, demonstrates that repairability and security can coexist. This research adds to the growing literature on repair in the information science space and how it is a cause for social justice initiatives (Centivany, 2024a,b). It highlights that a more inclusive and transparent regulatory approach is essential to counter undue industry influence and uphold public welfare in the evolving technological landscape.

References

Alliance for Automotive Innovation v. Healey, Complaint, No. 1:20-cv-12090 (D. Mass. Nov. 20, 2020)

Ballotpedia. (2020). *Massachusetts question 1, "right to repair law" Vehicle data access requirement initiative (2020).* https://ballotpedia.org/Massachusetts_Question_1,_%22Right_to_Repair_Law%22_Vehicle_Data_Access_Requirement_Initiative_(2020)

Banner, J. (2023, June 16). *Access denied: NHTSA instructs automakers to ignore Massachusetts Data Access Law*. MotorTrend. https://www.motortrend.com/news/nhtsa-massachusetts-data-access-law-right-to-repair/

Bill C-244, An Act to amend the Copyright Act (diagnosis, maintenance and repair), 44th Parliament, Received Royal Assent November 7th 2024.

Blanco, S. (2023, January 30). *Tesla EVs, even mildly damaged, are being written off by insurance companies*. Car Driver. https://www.caranddriver.com/news/a42709679/tesla-insurance-fixes-expense/

Caltrider, J., Rykov, M., & Macdonald, Z. (2023, September 6). *privacy not included: A Buyer's guide for Connected Products. Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

Canada, Parliament, House of Commons, Standing Committee on Industry and Technology. (2023, January 20). *Minutes of Proceedings*, 44th Parliament, 1st Session, Meeting No. 57. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/44-1/INDU/meeting-57/minutes

Centivany, A. (2023, March). Testimony on *Bill C-294: An Act to Amend the Copyright Act (interoperability)* before the House of Commons Standing Committee on Industry & Technology.

Centivany, A. (2023, February). Testimony on *Bill C-244: An Act to Amend the Copyright Act (diagnosis, maintenance, and repair)* before the House of Commons Standing Committee on Industry & Technology.

Centivany, A. (2024, October). Testimony on *Bill C-244: An Act to Amend the Copyright Act (diagnosis, maintenance, and repair)* before the Senate Standing Committee on Banking, Commerce, and the Economy.

Centivany, A. (2024). "You Are Not Here": Coordinating Repair under Occupation. *Proceedings of the Association for Information Science and Technology*, 61(1), 80-91.

Dal Bó, Ernesto. "Regulatory capture: A review." *Oxford review of economic policy* 22, no. 2 (2006): 203-225.

DRI Faculty List. (2017). https://www.dri.org/docs/default-source/event-brochures/2017/strictly-automotive/20170201-speaker-list.html?sfvrsn=10

Ekman, E. (2019, November 20). *Here's one reason the U.S. military can't fix its own equipment*. The New York Times. https://www.nytimes.com/2019/11/20/opinion/military-right-to-repair.html

Exec. Order No. 14036 (2021, July 9th). The White House "Executive Order on Promoting Competition in the American Econom.", https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promotingcompetition-in-the-american-economy.

Fairclough, N. (2013). Critical discourse analysis. In *The Routledge handbook of discourse analysis* (pp. 9-20). Routledge.

Fillman, E. (2023). Comprehensive Right to Repair: The Fight against Planned Obsolescence in Canada. *Dalhousie J. Legal Stud.*, *32*, 123.

Forno, R. (2021, January 8). *Challenging cybersecurity as the reason to oppose the consumer right to repair*. Center for Internet and Society. https://cyberlaw.stanford.edu/blog/2021/01/challenging-cybersecurity-reason-oppose-consumer-right-repair

Gault, M. (2023, August 29). *Right-to-repair advocates tore down a McFlurry machine to show it's actually easy to fix*. VICE. https://www.vice.com/en/article/g5ydey/ifixit-tore-down-a-mcdonalds-mcflurry-machine-to-prove-its-easy-to-repair

Grinvald, L. C., & Tur-Sinai, O. (2021). The right to repair: perspectives from the United States.

Iacurci, G. (2023, July 25). *Car repair costs are up almost 20% over the past year. here are 6 reasons why*. CNBC. https://www.cnbc.com/2023/07/25/car-repair-costs-are-up-almost-20percent-over-the-past-year-heres-why.html

Is There A Right To Repair?: Hearing Before the U.S House Judiciary Subcommittee on Courts, Intellectual

Kerry Kolodziej (n.d.). [LinkedIn page]. LinkedIn Retrieved April 7th, 2024 from https://www.linkedin.com/in/kerry-kolodziej-83941311/

Koebler, J. (2018, November 15). "I'm Possibly Alive Because It Exists:" Why Sleep Apnea Patients Rely on a CPAP Machine Hacker. VICE. https://www.vice.com/en/article/xwjd4w/im-possibly-alive-because-it-exists-why-sleep-apnea-patients-rely-on-a-cpap-machine-hacker

Kolodziej, K. E. (2023, June 13). [NHTSA Letter to Counsel for Vehicle Manufacturers to state concerns and conflicts between the Safety Act and the Data Access Law]

LaForest, A. (2020, December 5). *Auto Innovation Group flexes its lobbying muscles | automotive news*. Automotive News. https://www.autonews.com/regulation-safety/auto-alliance-flexes-its-lobbying-muscles

LaForest, A. (2023, May 26). *Automakers ask court to block June 1 enforcement of Mass. updated right-to-repair law*. Automotive News. https://www.autonews.com/service/automakers-rush-block-enforcement-mass-right-repair-law

LAW360. (n.d.). *Kerry E. Kolodziej, Mayer Brown*. https://www.law360.com/firms/mayer-brown/attorneys/kerry-e-kolodziej/cases

Li, W. Y. (2023). Regulatory capture's third face of power. *Socio-Economic Review*, *21*(2), 1217-1245.

Lowery, L. (2023, August 24). *NHTSA & Mass.. Ag Say Bluetooth could be answer to Data Access Law Compliance*. Repairer Driven News. https://www.repairerdrivennews.com/2023/08/24/nhtsa-mass-ag-say-bluetooth-could-be-answer-to-data-access-law-compliance/

Marshall, A. (2023, August 23). *A controversial right-to-repair car law makes a surprising U-Turn*. Wired. https://www.wired.com/story/nhtsa-massachusetts-right-to-repair-letter/

Mass. Gen. Laws Chapter 93K, § Section 2. 2013. Retrieved from https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93K/Section2

Mirr, N. A. (2019). Defending the right to repair: An argument for federal legislation guaranteeing the right to repair. *IowA L. REv.*, *105*, 2393.

Montello, S. K. (2020). The right to repair and the corporate stranglehold over the consumer: Profits over people. *Tul. J. Tech. & Intell. Prop.*, *22*, 165.

Moore, D. (2018). You gotta fight for your right to repair: The Digital Millennium Copyright Act's effect on right-to-repair legislation. *Tex. A&M L. Rev.*, *6*, 509.

Perzanowski, A. (2020). Consumer perceptions of the right to repair. *Ind. LJ*, *96*, 361.

Roberts, P. F. (2023, June 21). *Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity*. Forbes. https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=6ade922c428b

Samsung (n.d.). Use Maintenance mode on your Galaxy phone or Tablet. https://www.samsung.com/us/support/answer/ANS00091542/

Schneier, B. (2008, June). The psychology of security. In *International conference on cryptology in Africa* (pp. 50-79). Berlin, Heidelberg: Springer Berlin Heidelberg.

Stanton, C. (2022, December 30). *Do you have the right to repair your phone?*. Intelligencer. https://nymag.com/intelligencer/2022/12/the-right-to-repair-movements-biggest-battle.html

Stone, M. (2023, January 11). *A Massachusetts law protects the right to repair your own car. automakers are suing.* Grist. https://grist.org/transportation/a-massachusetts-law-protects-the-right-to-repair-your-own-car-automakers-are-suing/

Waldman, P., & Mulvany, L. (2020, March 5). *Farmers fight John Deere over who gets to fix an $800,000 Tractor*. Bloomberg.com. https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor

Warren, E. & Markey, E. (2023, June 15th). [Letter To Secretary Buttigieg and Deputy Administrator Schulman].

Zheng, W. (2014). The Revolving Door. *Notre Dame Law Review.* 90 1265-1308