CANADIAN REPAIR COALITION

www.canrepair.ca

Flipping the Narrative on Automotive Security

Manufacturers cannot hide behind scare tactics to restrict repair data for local shops and car owners

4 March 2024

Jasvinder Mann, Alana Baker & Dr. Alissa Centivany

As Canada grapples with the ever-concerning rise in automotive thefts tied to organized crime networks, broader themes of security, innovation, and the accountability of industries in the digital age have emerged.

Claims from vehicle manufacturers that allowing the right to repair will perpetuate car thefts and work against their efforts to keep vehicle systems secure are reflective of a revolving strategy of deflection, denial and distortion, rather than addressing the root causes of vulnerabilities. Similarly, considering a ban of cybersecurity testing devices like the Flipper Zero without a thorough understanding of their functions and benefits, are counterproductive.

The right to repair is about ensuring independent repair and service technicians have access to necessary data strictly for the diagnosis, service or repair of a product. If providing independent technicians with access to necessary vehicle data would compromise security, this suggests that the vehicle was not designed with security in mind from the outset.

By pinning the blame on external factors, manufacturers are diverting attention from their own shortcomings in securing products against theft and other forms of unauthorized access. While offering a temporary reprieve for the industries in question, this strategy does a disservice to consumers, policymakers, and the broader ecosystem of innovation and security.

Manufacturers must be held accountable for the security vulnerabilities of their products, and there needs to be a clear delineation between security measures and the legitimate interests of interoperability, repair, and research.

Security through obscurity is not good enough for Canadians. It is imperative that we demand evidence-based policy-making that distinguishes between legitimate security concerns and unfounded fears.

A recent controversy in Canada has ignited a debate that touches on the immediate issue of automotive theft and upon broader themes of security, innovation, and the accountability of industries in the digital age. The debate centers around the Flipper Zero, which is a multi-tool device designed for security researchers and hobbyists, which allows for interaction with a wide range of digital protocols and systems, such as RFID, NFC, and GPIO pins.[1,2] Its primary function is to test and explore digital systems for vulnerabilities, thereby aiding in the identification and remediation of security risks. Though the Flipper Zero is not the only device of its kind, it has been vilified as a tool for car thefts, prompting the federal government to consider its ban. This situation, however, reveals a more complex narrative about the scapegoating of technology, the responsibilities of manufacturers, and the need for a nuanced approach to policy-making in the face of technological advancements.

The federal government's decision to ban the Flipper Zero came after a meeting on automotive theft, where industry representatives, without providing concrete evidence, claimed that the device facilitates auto theft. This move to outlaw the Flipper Zero is symptomatic of a reactionary approach to policy-making, where the solution offered is disproportionately simplistic and misdirected. The real issue at hand is not the device itself, which, as security experts have pointed out, is not a threat. COO of Flipper Devices Alex Kulagin has also mentioned that "Flipper Zero can't be used to hijack any car, specifically the ones produced after the 1990s, since their security systems have rolling codes".[3] The Flipper Zero possesses limited capabilities in terms of systems hacking. It is, instead, a valuable tool for those in the security space and your everyday person who likes to tinker with technology to identify vulnerabilities and promote remediation.

The controversy surrounding the Flipper Zero is emblematic of a broader pattern of behavior exhibited by the automotive industry and mirrored in other sectors, such as agriculture and consumer electronics. Faced with legitimate security concerns stemming from their products, these industries have historically opted for a strategy of deflection rather than addressing the root causes of vulnerabilities. By pinning the blame on external factors,

like the Flipper Zero, the industry diverts attention from its own shortcomings in securing products against theft and other forms of unauthorized access. This tactic of finding a scapegoat not only absolves the industry of the immediate need to enhance the security of its products but also stifles the discourse on interoperability and the ethical dimensions of technological research and disclosure.

While offering a temporary reprieve for the industries in question, this strategy does a disservice to consumers, policymakers, and the broader ecosystem of innovation and security. The focus on banning a tool like the Flipper Zero, based on panic, prevents meaningful engagement with the underlying issues of product security and the ethical use of technology. It perpetuates a cycle of fear-mongering and moral panic that obscures the real challenges and opportunities presented by technological advancements. This is also highlighted in the NHTSA's letter to Automakers in Massachusetts. When Massachusetts was trying to enact right to repair legalisation in the automotive sector the NHTSA felt compelled to right a letter essentially stating that giving telematic data to repair shops could be a safety concern.[4] With enough pushback, the NHTSA reversed their decision and allowed wireless access to data within a short distance.[5]

The implications of this Flipper Zero controversy extend beyond the immediate context of automotive theft, reflecting a systemic issue in how we conceptualize and respond to technological challenges. The narrative constructed around the Flipper Zero is part of a larger debate on how industries should be held accountable in the digital age and the role of policy in fostering an environment where technological advancements are leveraged for the public good while mitigating their potential harms. To move forward, it is imperative that we demand evidence-based policy-making that distinguishes between legitimate security concerns and unfounded fears. Industries must be held accountable for the security vulnerabilities of their products, and there needs to be a clear delineation between security measures and the legitimate interests of interoperability, repair, and research. This requires a collaborative approach that involves stakeholders from across the spectrum, including industry representatives, security experts, policymakers, and the public, to ensure that the solutions proposed are practical and conducive to the public's interests. Moreover, the discourse on technology and security must evolve to recognize the

complexity of the digital landscape. Simplistic solutions, such as banning a device without a thorough understanding of its functions and benefits, are counterproductive, and we encourage the government to do better.

---

[1] Rose, Janus. "Feds Want to Ban the World's Cutest Hacking Device. Experts Say It's a 'Scapegoat.'" VICE, February 12, 2024. https://www.vice.com/en/article/4a388g/flipperzero-ban-canada-hacking-car-thefts.

[2] "Flipper Zero - Portable Multi-Tool Device for Geeks." FLIPPER. Accessed February 16, 2024. https://flipperzero.one/#:~:text=Flipper%20Zero%20is%20a%20versatile,SPI%2C%20I2C%2C%20etc%20adapter.

[3] Kan, Michael. "Canada to Ban Flipper Zero Devices over Car Thefts." PCMAG, February 9, 2024. https://www.pcmag.com/news/canada-to-ban-flipper-zero-devices-over-car-thefts.

[4] Roberts, Paul F. "Tilting against Repair Law, NHTSA Endorses Security through Obscurity." Forbes, June 22, 2023. https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsaendorses-security-through-obscurity/?sh=7e1338dd428b.

[5] Walz, Eric. "US Regulators Approve Massachusetts Right-to-Repair Law." Automotive Dive, August 24, 2023. https://www.automotivedive.com/news/NHTSA-massachusettsright-to-repair-law/691743/.