ELECTRONIC FRONTIER FOUNDATION

January 13, 2020

RE: HB4122 (Automotive Right to Repair Bill)

_____
Massachusetts House of Representatives

Dear _____,

I write today in support of HB4122, the Automotive Right to Repair Bill. I am a Visiting Professor of Computer Science at the UK Open University and a Research Affiliate at the MIT Media Lab, and am a campaigner for digital rights, serving as a special consultant to the Electronic Frontier Foundation, a national, member-supported nonprofit that has advocating for digital rights since its founding in Massachusetts in 1990.

The case for amending Massachusetts' existing Right to Repair regime is clear: the original 2012 measure passed with overwhelming support (86%), but in the years since, the highly concentrated automotive sector has circumvented the spirit of that measure by redesigning their products to subvert Bay Staters' ability to fix their own cars or take them to independent mechanics.

The manufacturers accomplished this subversion by designing their informatics systems to transmit diagnostics using proprietary wireless interfaces -- which will be present in 90% of cars by 2022 -- that neither consumers nor independent mechanics can readily intercept and decode. Passing HB4122 will amend the Right to Repair regime and ensure that drivers will be able to make their own choices about which mechanics they trust to fix their cars best and at the best price, subjecting auto manufacturers' own repair divisions to much-needed market discipline, forcing them to win their customers' repair business rather than corralling those drivers into manufacturer-approved service depots.

Auto manufacturers have argued that independent service endangers drivers' cybersecurity. In reality, the opposite is true: security is weakened by secrecy and strengthened by independent testing and scrutiny. It is an iron law of information security that "there is no security in obscurity" -- that is, security cannot depend on keeping defects a secret in the hopes that "bad guys" won't discover and exploit those defects. And since anyone can design a security system that they themselves can't imagine any way of breaking, allowing manufacturers to shroud their security measures in secrecy doesn't mean that their cars can't be hacked -- in fact, history has shown that vehicle computers depending on secrecy for security are, in fact, frequently vulnerable to hacking.

815 Eddy Street, San Francisco, CA 94109 USA **phone** +1.415.436.9333 **fax** +1.415.436.9993 **email** info@eff.org **eff.org**

In 2018 and 2019, cities, hospitals, and other large institutions had their informatics systems seized by petty criminals using off-the-shelf ransomware that had combined with a defect in Windows that the NSA had discovered and kept secret -- until an NSA leaker released it to the world. As these cities discovered, the NSA's decision to keep these defects secret did not put them out of reach of bad guys -- it just meant that institutional Microsoft customers were put at grave risk, and that Microsoft itself did not know about the devastating bugs in its own products and so could not fix them.

Information security is absolutely reliant upon independent security researchers probing systems and disclosing what they discover. Allowing car manufacturers to monopolize service -- and thus scrutiny -- over their products ensures that the defects in these fast-moving, heavy machines will primarily become generally known *after* they are exploited to the potentially lethal detriment of drivers and the pedestrians around them.

The manufacturers' desire to monopolize bad news about design defects in their own products is especially dire because it rides on the tails of a strategy of monopolizing service and parts for those products. The uncompetitive, concentrated automotive sector has already brought itself to the brink of ruin -- averted only by the infusion of $80.7B in tax-funded bailouts. More than a decade later, it remains in dire need of competitive discipline, as is evidenced by a commercial strategy dominated by reducing public choice, surveilling their own customers and selling their data, and extracting monopoly rents from luckless drivers who are locked into their proprietary ecosystems.

I would be delighted to speak further with you about this at your convenience.

Sincerely,

Dr Cory Doctorow
Special Consultant, Electronic Frontier Foundation
Visiting Professor of Computer Science, Open University
Research Affiliate, MIT Media Lab
Visiting Professor of Practice, University of North Carolina School of Library and Information Science