Anthony D Rosborough*

SOURCE CODE

A Trade-Related Barrier to the Right to Repair

* Assistant Professor of Law & Computer Science, Dalhousie University (Canada); Doctoral Researcher in Law, European University Institute (Italy), anthony.rosborough@dal.ca

HEINRICH BÖLL STIFTUNG
WASHINGTON, DC
USA | Canada | Global Dialogue

TACD Trans Atlantic Consumer Dialogue

HEINRICH BÖLL STIFTUNG
BRUSSELS
European Union | Global Dialogue

Acknowledgements

ABOUT THE AUTHOR

Anthony D Rosborough is an Assistant Professor of Law and Computer Science at Dalhousie University (Canada). He obtained his LLM from the University of Glasgow and PhD from the European University Institute (Italy).

Anthony teaches and writes at the intersection of ubiquitous computing, intellectual property law, regulatory theory, and science and technology policy. His research is focused on the Right to Repair movement and open innovation.

As a frequent commentator on Right to Repair and related industrial policies, Anthony has provided expert testimony and advice to Canada's Standing Committee on Industry and Technology, the European Parliament, the European Commission, the United States Librarian of Congress, and the Australian Productivity Commission. He has appeared on numerous radio and television programs around the world in relation to intellectual property, trade, market competition, and Right to Repair issues.

Report commissioned by TACD, the Transatlantic Consumer Dialogue. Research for this report was made possible with the support of the Heinrich-Böll-Stiftung European Union | Global Dialogue & Heinrich-Böll-Stiftung Washington, DC USA | Canada | Global Dialogue

December 2025

Table of Contents

Executive Summary

In recent years, conflicts between software access restrictions and Right to Repair (R2R) legislation have become a growing concern for policymakers and repair advocates around the world. Consumers have come to increasingly depend on electronic devices that integrate sophisticated hardware and embedded software. When those devices break or require maintenance, owners often lack the software or software-based tools required to fix them. In some cases where replacement parts and information may be readily available, device software and software-integrated tools present a barrier to independent repair. In response, legislators in both the United States and the European Union have been enacting R2R laws designed to empower consumers and professional repairers with access to these resources to foster a circular economy and reduce electronics waste.

At the same time, trade negotiators on both sides of the Atlantic have been concluding free trade agreements (FTAs) that include digital trade provisions that protect software source code and algorithms from inspection and disclosure by governments or access by third parties. These provisions, such as those found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the US-Mexico-Canada Agreement (USMCA) and subsequent EU-led agreements, bar governments from requiring device manufacturers to transfer or disclose source code or algorithms as a condition for market access.[1]

Though to date these parallel policy developments have (for the most part) occurred in isolation from one another, this report examines their potential for interaction and future conflict as contemporary FTAs and R2R mandates with software disclosure obligations come into effect. These seemingly distinct legal and policy developments may come into conflict where, for example, R2R mandates explicitly or implicitly require manufacturers to transfer or provide access to source code or algorithms for the benefit of third-party repairers or consumers.

Drawing from statutory texts, recent trade agreements, policy briefs, and media reports, the study assesses the importance of access to software tools for repair, analyses domestic R2R legislation in the United States and Europe, surveys source-code provisions in major agreements, evaluates potential conflicts, and offers recommendations for policy makers. The report's key findings are that:

t initialize.context.createBuffer({id: “genesis_0x7f4b”, type: “VERTEX”, size: 2048,fo
utes: [{ name: ‘a_position’, offset: 0, stride: 12 }, { name: ‘a_normal’, offset: 12,
onst artifactMesh = await initialize.context.createBuffer({id: “genesis_0x7f4b”, type: “VERTEX”, size: 2048,fo
rmat: ‘vec3<f32>’, attributes: [{ name: ‘a_position’, offset: 0, stride: 12 }, { name: ‘a_normal’, offset: 12,

Repair now depends on software. Parts pairing, diagnostic software, firmware[2] updates, and calibration tools are now essential repair resources. Both EU and U.S. R2R frameworks explicitly recognise that access to these software-based tools is as critical as access to parts and manuals. Recent EU legislation[3] and some U.S. state laws (New York, Minnesota, Colorado) impose obligations on manufacturers to provide repair-related software to third parties. In Europe this includes the Directive on common rules promoting the repair of goods (“R2R Directive”)[4], the EcoDesign for Sustainable Products Regulation (“ESPR”)[5], and the EcoDesign Regulation for Smartphones and Tablets (“ERST”)[6]. U.S. state-level R2R laws include those passed in New York[7], Minnesota[8], and Colorado[9]. These obligations stop short of requiring explicit access to source code, but they cover keys and utilities that could be legally construed as such.

FTA source code secrecy provisions create friction. Agreements like USMCA, CPTPP, and EU-Japan EPA prohibit governments from requiring access to source code (and in some cases algorithms). Depending on their interpretation, manufacturers may invoke these clauses to resist obligations under R2R laws that require provision of software tools or firmware to third parties, even if those obligations target primarily object code or binaries.

Treaty language diverges in restrictiveness. Agreements like the USMCA adopt broad protections for source code and algorithms with only narrow, case-by-case exemptions, whereas newer EU-led agreements provide more permissive exceptions for regulatory oversight and public policy objectives. This variation creates uncertainty for R2R enforcement and potential conflicts.

Shifting policy positions present an opportunity for change. In late 2023, the U.S. reversed its prior stance on digital trade and source code secrecy rules at the WTO, citing the need to preserve domestic regulatory space (including the R2R). The EU’s digital trade agenda continues to advance source code secrecy rules but with increasingly explicit exceptions and public-interest acknowledgements. This indicates a possible convergence around a more balanced approach that accommodates both digital trade and R2R objectives, signalling an opportunity to revisit these rules and their impacts.

1. Introduction

1.1 Context and Background

Demands for greater product repairability and durability can be traced back many decades[10], but the modern R2R movement's genesis is situated in the early 2000s, stemming largely from within the automotive sector.[11] The movement has since expanded widely into the realms of consumer electronics, home appliances, commercial and industrial equipment[12], and even critical infrastructure.[13] In essence, R2R advocates argue that consumers and independent repair technicians should have reasonable access to the parts, tools, and information needed to fix the products that they own. Proponents highlight environmental benefits (reduced waste and carbon emissions), economic advantages (lower repair costs and increased market competition), and social benefits through the diffusion of technical knowledge and information sharing. In the EU, the United States, and beyond, R2R advocates have found enormous success in passing laws and policy that helps achieve these goals in various ways.

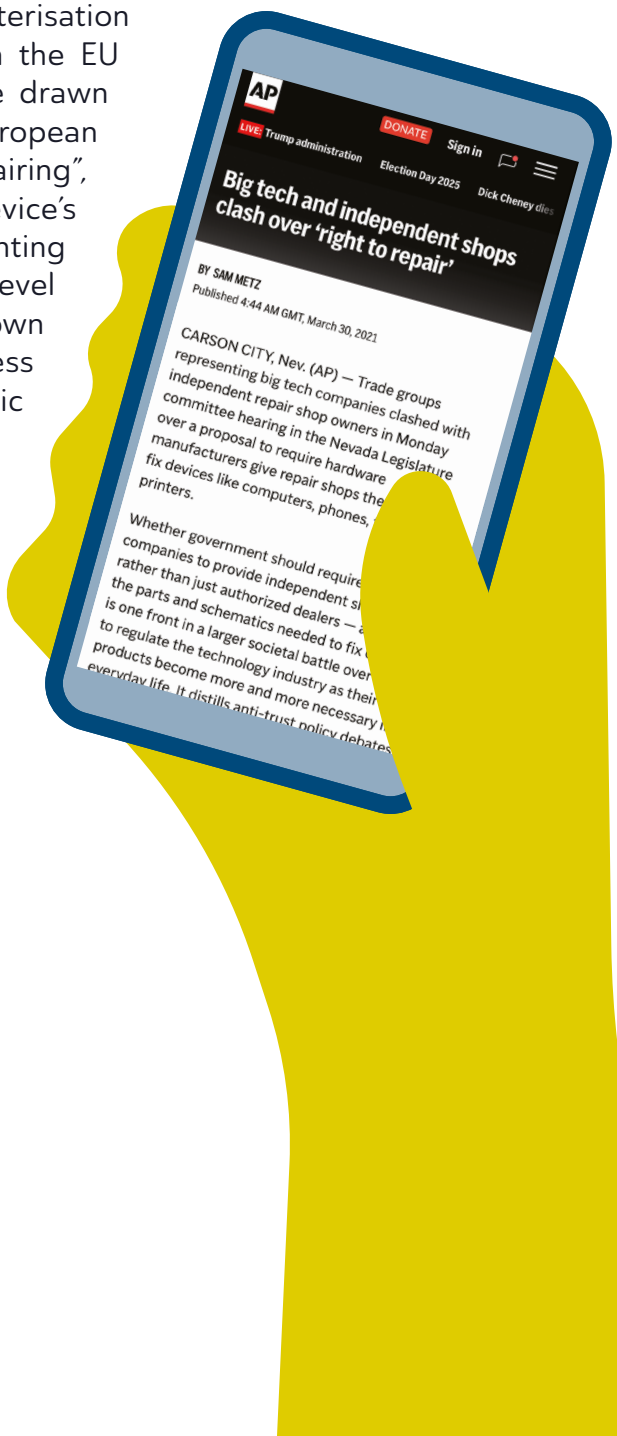
Key to this success has been the movement's open and flexible norm in pushing for a right to repair. This permits several complementary policy approaches that fall under the movement's umbrella. In broad terms, these approaches can be placed into two broad categories of negative rights and positive rights.[14] The negative right approach involves reducing legal and regulatory barriers to independent and self-repair. This results in a focus on establishing new exceptions and limitations to various intellectual property rights, preventing manufacturers from voiding warranties following independent repairs, and emboldening market competition or anti-trust authorities with greater enforcement mechanisms. In essence, the negative rights approach to the R2R is motivated by the pursuit of various individual and consumer freedoms.

The positive right approach, on the other hand, involves imposing new obligations on manufacturers to provide consumers and independent repairers with the necessary parts, tools, and information to complete repairs at a reasonable cost. In this way, it is focused primarily on securing various entitlements. This ordinarily involves amendments to consumer laws and the establishment of new and bespoke enforcement and compliance mechanisms to ensure that manufacturers follow prescriptive requirements as to the design of products and their support for consumers after sale.

Importantly, positive rights approaches to the R2R ordinarily impose ongoing obligations to provide replacement parts, information, and tools (including software) to consumers after the point of sale. Though R2R schemes in the EU and across United States differ in some respects, they commonly share these aspects of a positive rights approach, including mandated access to diagnostic software, firmware, and software-based tools in relation to various devices and products.

1.2 The Essential Role of Software for the Right to Repair

The increasing focus on software and software-based tools for repair practices is in response to the widespread computerisation and software-dependency of products and devices. Both the EU and United States' recent R2R policy developments have drawn attention to these dynamics. In late 2023, for example, the European Parliament approved a set of measures banning "parts pairing", a software-based product design practice where a device's components are digitally linked to its serial number, preventing third-party or self-repair (even with genuine parts).[15] State-level R2R bills in the United States in recent years have also shown an emphasis on forcing manufacturers to provide access to embedded software and the means to 'reset electronic security locks'.[16]



The R2R movement's emphasis on software disclosure obligations has been (unsurprisingly) met with pushback from manufacturers. This is largely due to the crucial role that software and software-based product controls play in protecting business models and exclusive supply chains. In legislative debates, hearings, and

public pronouncements relating to the R2R, manufacturers have often opposed disclosure of software-tools in particular[17], countering that restricting access is necessary to prevent intellectual property infringement, tampering with products, or ensuring public safety or compliance with other regulatory requirements.[18] In a few instances, manufacturers have sought to resist, narrow, or find alternative pathways to mandated disclosure or access to their software and software-based tools, whether through litigation or voluntary agreements with independent repairers on manufacturers' terms.[19]

1.3 Growing Friction with International Trade

Against this backdrop, the international trade realm has been gradually introducing a new potential constraint on mandated disclosure and access to software as part of R2R policy. Over the last decade, a "no-forced disclosure" template for software has spread through FTAs' "digital trade" chapters. These sections, typically titled "source code", prohibit governments from requiring access to, or transfer of, source code and increasingly "algorithms" (often ambiguously defined). In some cases, this prohibition is narrowed to situations where transfer or access is required for market entry, while in more recent agreements the prohibition is general and potentially more expansive. These new rules are often subject to only narrow case-by-case exceptions that do not envision comprehensive and perpetual regulatory frameworks like the R2R.

Though this special source code protection in FTAs was orchestrated to protect trade secrets and cybersecurity amidst geopolitical rivalry and tensions, the net effect is to elevate software secrecy from a matter of domestic private law into an international commitment. Even where R2R frameworks may have strong public-interest dimensions, the presence of these new rules may provide well-resourced firms with a new avenue, forum, and vocabulary to resist or narrow R2R mandates that oblige provision of software and software-based tools. And though R2R frameworks may not explicitly require disclosure of human-readable source code, manufacturers may nevertheless argue that compelled provision of tools, programs, firmware, or keys exposes protected logic or amounts to a de facto disclosure of algorithms.

There is a tension at play in that R2R mandates treat software as a necessary instrument of product maintenance and consumer choice, while contemporary

FTAs treat software as a sensitive asset to national security that must be insulated from mandatory disclosure to third parties. As the EU and the United States move from high-level principles to more concrete and enforceable duties on software tools and anti-pairing measures, friction with FTA source code protection clauses is inevitable. That friction will be felt most acutely in sectors where embedded software governs core device functions with potential safety implications if accessible by third parties. Friction will also be felt where manufacturers rely on proprietary software ecosystems to deliberately prevent third-party repair and servicing of their products and devices and protect exclusive business models.

1.4 Report Roadmap

The purpose of this report is to identify the areas of potential tension between domestic R2R frameworks and emerging FTA source code protections. This includes offering recommendations to chart a successful path forward for R2R policy and recalibration of overbroad trade rules on both sides of the Atlantic. Accordingly, Section 2 lays out the practical role of software in repair activities, showing its role in calibration of devices following physical repair, diagnostic scans and reading fault codes, and firmware updates. Section 3 then analyses a selection of recent R2R policy developments in the EU and United States that show a strong emphasis on software and software-based tools, including U.S. state-level bills covering consumer electronics and the EU's R2R Directive and the ESPR. Section 4 explains the origins and history of FTA source code protections before examining a selection of treaty language from recently concluded agreements to exemplify the overall trend and approach. Section 5 then explores the potential areas of conflict and tension between FTA source code protections at the international trade level and domestic R2R frameworks in the United States and EU. Finally, Section 6 concludes with a series of conclusions and recommendations for policymakers and trade representatives.

2. The Practical Role of Software in Repair Activities

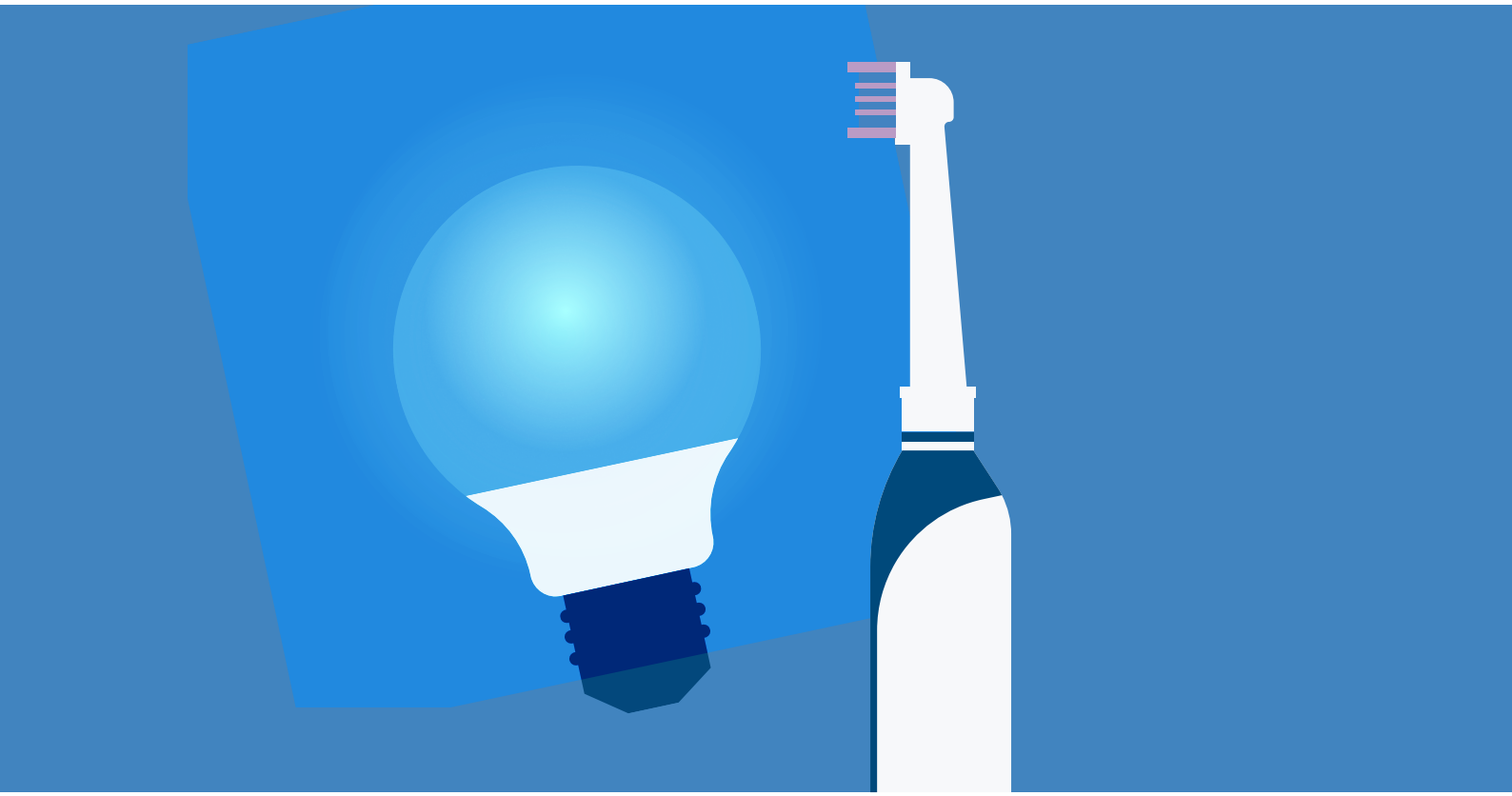
Modern electronically enabled devices and products are increasingly software-dependent, and this fundamentally changes the landscape of repair and maintenance. In the past, repairing a device might have involved simply swapping purely mechanical parts or soldering components, with minimal need for supplementary software or software-enabled tools.

Today, however, everything from smartphones and laptops to cars, farm tractors, and even medical devices contain embedded computers and software. This radically changes repair practices, the knowledge and skills required to carry them out, and the tools and resources needed to complete them properly.

This trend is part and parcel of the proliferation of "ubiquitous computing", a design paradigm where computing appears seamlessly anytime and everywhere, embedded into a wide range of devices and products through smaller and more energy efficient hardware.[20] Ubiquitous computing is closely related to the broader Internet-of-Things (IoT) concept. This refers to a network of physical objects ("things") with embedded computer hardware, sensors, and other technologies that exchange data with other devices and systems over the internet or other communications networks.[21]

At the end of 2024, there were approximately 18.8 billion connected IoT devices globally, marking a 13% increase from the year prior. Projections indicate that this number will more than double (reaching over 40 billion) by the year 2030.[22] Beyond these facts and figures however, the growth of software-dependent devices can be observed in more anecdotal terms. Seemingly every product – from toothbrushes to home appliances – is now packaged with "smart" or connected features of one kind or another. These technological shifts mean that fixing a hardware problem frequently requires access to software, firmware, or digital keys that are often only made available through the manufacturer's supply chain or network. Across a wide range of product categories, consumers and independent technicians frequently find that software and software-based tools are as critical as screwdrivers in a repair toolkit.[23]

The following sections break down several key categories in which software, firmware, and software-enabled tools play a pivotal role in repairing and maintaining a variety of electronic devices. These are broken down into categories that share considerable overlap but generally fall along the lines of replacing physical parts, diagnosing errors and faults, and calibrating or fine-tuning equipment following repairs. For each category, product examples are provided to illustrate how software bottlenecking manifests in both consumer electronics repair and other technologies (with parallels in both the EU and United States contexts).



2.1 Parts-Pairing and Software Locks

Parts-pairing refers to the practice of electronically linking a replaceable component to the device via onboard software, so that the device will recognise only an 'authorised' part. In practical terms, manufacturers embed microchips or serial numbers in components and program the device's firmware to verify those identifiers. If a part's ID does not match the device's expected identifier (for example, because the user installs a replacement part from another device), the onboard software may refuse to fully operate or may disable certain functions without authorisation by official software.

This approach to device and component design should be familiar to owners of consumer grade printers, which often have systems to detect whether replacement ink cartridges are 'authentic'. Parts-pairing refers to a broader and more robust implementation of this system design approach to encapsulate many of a device's physical components, rendering many repairs dependent on specialised software that is not ordinarily made available to end-consumers. This tends to undermine self-repair and independent shops and refurbishers by presenting error messages or lost features following successful physical repairs.

2.1.1. Parts-Pairing in Apple's Smartphones

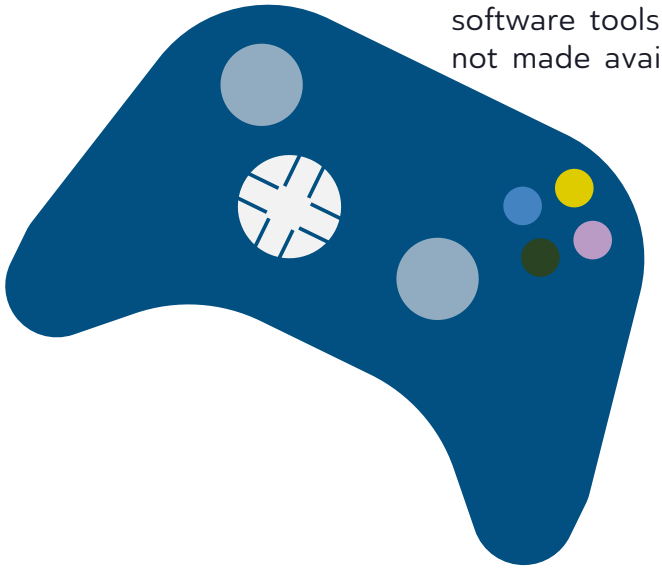
Likely the most well-known (and widely reported) example of parts-pairing is in relation to Apple's line of smartphones. iPhones manufactured in recent years have multiple serialised components (screens, batteries, cameras, Touch ID/Face ID sensors). If, for example, a consumer or unauthorised repairer attempts to replace a broken iPhone display or a worn-out battery, the phone's onboard software will detect the new part's serial mismatch. As a result, certain features will stop working and warning messages will appear. For instance, the ambient light auto-adjust feature (known as "True Tone") is disabled after a screen swap, and the system will persistently warn that it 'cannot verify' a non-genuine display or battery.[24] Even more critically, an authorised swap of an iPhone's Touch ID or Face ID module may outright break those biometric login features for security reasons.

The consequence of these parts-pairing techniques is that only Apple (or an Apple-authorised technician) has the software tools to reset parts-pairing by resetting the serial numbers of replacement parts. The tight grip kept on these software tools by Apple has caused independent repair shops to lose business, as customers understandably are less interested in repairs that result in degraded functionality or incessant 'genuine part' warnings after repair.[25] As a result, many R2R advocates have flagged Apple's parts-pairing design and unwillingness to share software tools as a deliberate strategy to monopolise repairs.

Following increasing pressure on lawmakers by R2R advocates to ban these practices through legislation, Apple only recently announced a new on-device "Parts & Repair Assistant" application that will allow owners of iOS 18 and newer iPhones to pair used genuine parts (from donor devices) for certain iPhone models without specialised equipment.[26] While an important step for the R2R, parts-pairing practices are still widely used by Apple outside of its line of smartphones, highlighting the enduring and crucial role of external software tools to complete physical repairs.

2.1.2. Game Consoles and the Automotive Industry

Parts-pairing is also prevalent across a broader range of consumer electronics, including game consoles. A notable case of this is the Microsoft Xbox One. To combat game piracy and hardware tampering, Microsoft digitally paired each console's optical disc drive to its motherboard at the factory. The console's firmware checks that the installed DVD/Blu-ray drive is the original upon each startup. If it is not, the console will refuse to play the game or media.[27] As Microsoft itself has explained, "If your Xbox One optical disk drive broke, you can't take someone else's optical disk drive and plug it in. It won't work. These two things have to be paired together and only our factories can pair them."[28] The effect of this is a significant impediment to independent repair, with one of the most failure-prone components (the disc reader) may render the entire device inoperable if it fails and the manufacturer's software tools are not made available.



The automotive industry has also begun to wrestle with the increasing prevalence of "VIN locking", a type of parts-pairing that presents barriers for independent automotive mechanics.[29] Despite the long history of modularity and interoperability in the automotive industry, VIN locking now enables manufacturers to digitally lock specific parts and components to a single vehicle.[30] This has become more prevalent with the rise of electric vehicles (EVs) which feature more robust layers of computerisation than their internal combustion predecessors. For independent automotive technicians, completing many physical repairs and parts replacements on modern vehicles requires access to the manufacturer's bespoke diagnostic tools and reprogramming protocols, which are often costly or difficult to obtain for smaller shops.

Cumulatively, these examples show that in modern devices the "tool" that makes physical parts replacement possible is supplementary software or keys/codes required to access and modify existing on-board software. Manufacturers serialise components and bind them (via firmware checks, cryptographic handshakes, or digital keys) to a specific device that replacements trigger warnings or lose functionality. In the end this means that completing a repair successfully typically requires access to software utilities in addition to analog tools and parts.

2.2 Diagnostic Software and Scan Tools

While parts-pairing reveals the importance of software for modifying physical components of devices, the role of diagnostic software and scan tools reveals the importance of software for understanding faults requiring repair at the outset. Many of today's devices and products are designed to detect faults and log error codes through onboard software.

When something goes wrong (be it a sensor failure, a motor issue in an appliance, or a malfunctioning circuit), the device's firmware may force the device into a reduced functionality state (sometimes referred to as "safe mode" or "limp mode") and/or display error messages.

Reading, understanding, and clearing these errors to restore full functionality are tasks that all commonly involve additional software tools or special keys or codes. As one might imagine, these types of diagnostic tools or codes are often not made widely available to consumers or independent repairers.

2.2.1 Taylor C602 Soft-Serve Machine (McDonald's Restaurants)

The Taylor C602 soft-serve ice cream machine (a standard in most McDonald's restaurants around the world) is a highly publicised example of how decisive software access is in diagnosing faults. The C602 periodically runs a complex thermal and pasteurization cycle for sanitisation purposes that frequently (and notoriously[31]) results in equipment failure.[32] Putting these ice cream machines back into operation requires navigating service menus, entering program codes known only by the manufacturer, as well as clearing specific error codes before the unit can operate properly again.

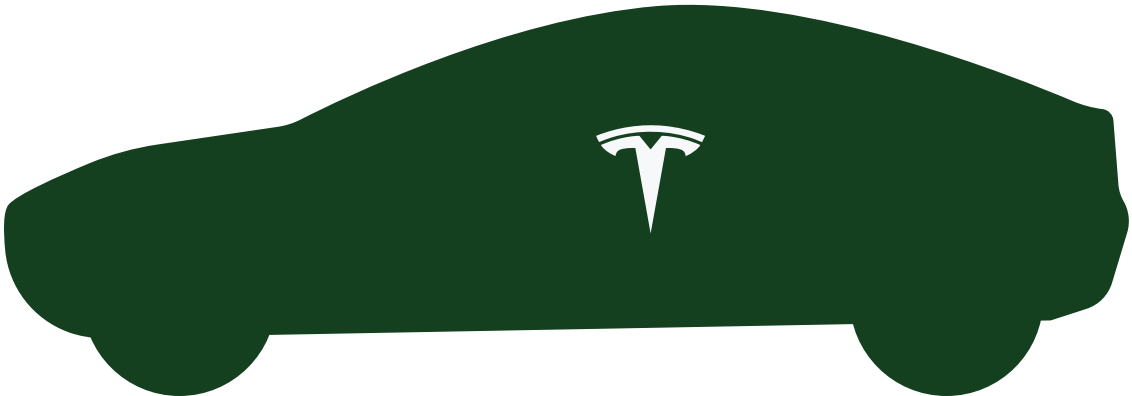
Crucially, much of these capabilities are kept secret or hidden from users and

McDonald's franchisees. These capabilities are also undocumented in publicly available user manuals and require special tools to access them, leaving Taylor with a de facto monopoly on repair and servicing.[33] The prevalence and global reach of this issue resulted in a technology startup Kytch producing a device that attaches to the internal control of the C602 to decode error messages and reroute diagnostic data over the internet to restaurant managers and operators, enabling better detection of issues and troubleshooting.[34] Development of this device later resulted in legal battles between Taylor, Kytch, McDonald's, and its franchisees, resulting in Taylor producing and selling its own version of the device.[35]

Overall, the C602 serves as a helpful example of the contention that diagnosis and understanding faults in computerised devices and equipment often requires special access to software logs, error codes, and hidden menus. This access is facilitated either through supplementary software, or special keys or codes to access and modify software already present on the device. Absent access to these resources, device owners and even skilled technicians are forced to deal exclusively with manufacturers' networks for repair and servicing.

2.2.2 "Tesla Toolbox" Diagnostic Software

Diagnostic tools have a lengthy history in the automotive industry, and over the last several decades the industry has settled on common formats and data protocols to provide vehicle owners and independent technicians with crucial repair information.[36] Despite this standardisation, however, many manufacturers have begun to implement more sophisticated and bespoke systems for diagnosing faults.[37] A cutting edge example of proprietary diagnostic software is Tesla's "Toolbox" platform. The network-connected diagnostic software communicates with the car's onboard computer for deep diagnostics, understanding faults, and to run tasks like controller resets and programming new components. Tesla originally withheld access to Toolbox for consumers and independent technicians entirely, leaving salvaged or modified Teslas often crippled or with reduced functionality. Following increased pressure from lawmakers and repair advocates, however, the manufacturer began offering paid access to the platform in 2021. Toolbox access is facilitated through a service subscription program with two tiers: one giving access to repair manuals and parts catalogs, and a higher tier unlocking diagnostics.[38] Tesla's Toolbox platform underscores how control over software tools can limit (in absolute fashion) the ability for consumers and independent technicians to diagnose faults and give effect to physical repairs.

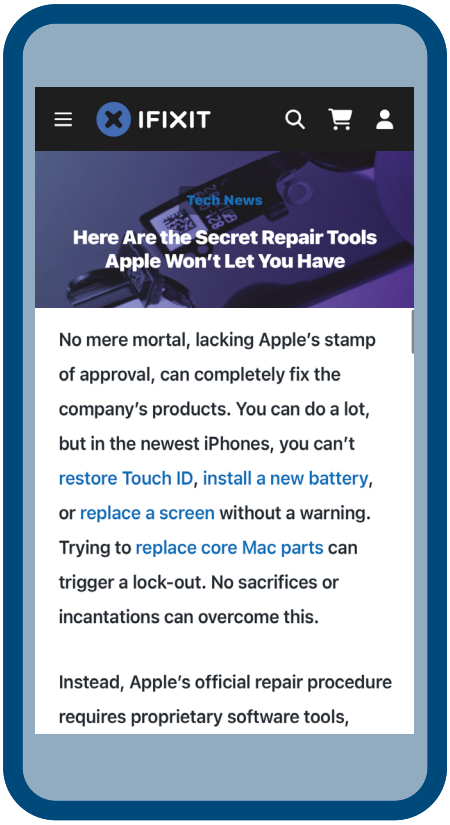


2.3 Calibration and Configuration

Closely related to parts-pairing, authenticating replacement parts, and diagnosing errors or faults, software also plays a key role in calibration or fine tuning of devices following successful physical repairs. Calibration processes like aligning a camera module or configuring a new battery's charging parameters are often the final step in a repair process.

2.3.1 Apple's "Service Toolkit 2" Calibration Software for iPhones

In addition to software needed to successfully pair replacement parts, modern smartphones also require software utilities for successful calibration and configuration. This is especially true for higher-end devices like Apple's iPhone. Apple historically used an internal iPhone calibration machine (known as the "Horizon Machine") to recalibrate components like the Touch ID fingerprint sensor after screen repairs.[39] Today, however, most calibration tasks on iPhones is carried out through software-only tools like Apple Service Toolkit 2 ("AST 2").[40] This is a cloud-based diagnostic platform and system configuration tool that finalises repairs. These tools perform tasks like True Tone display recalibration, battery health resets, and facilitate parts-pairing for replaced components.



In 2023, following increased pressure from pending R2R legislation, Apple released a tool to consumers as part of its "Self Service Repair" program with similar functionalities to AST 2. This allows users to initiate cloud calibration processes post-repair.[41] This iOS-based application, "Repair Assistant", downloads the necessary firmware/calibration data for components like screens, batteries, or Face ID modules.

It should be pointed out that Apple is not the only manufacturer to rely on specialised software tools for calibration of this sort. Other smartphone and laptop makers also use proprietary software (though often less publicised and well-known). Many Android manufacturers have internal diagnostics or firmware flash tools for their repair centres.[42] The technical roles are similar in that calibrating sensors, updating firmware, and clearing error codes often requires access to specialised software utilities. But Apple's calibration tool exemplifies the increasing sophistication of software-based utilities that are required as part of many repair processes, requiring active connection to the internet and an authorised account.

2.3.2. GE's "Smart HQ" Service Calibration Tool

GE's Smart HQ Service is a subscription diagnostic platform only made available for 'professional' technicians. It is used with a GE Bluetooth module that plugs into an appliance's service port jack and pairs with an enabled phone or tablet application.[43] Once connected, the app can read log data, calibrate components, and install firmware updates. GE sells the hardware module separately and charges an ongoing subscription for access to the software and cloud features.[44]

Smart HQ enables post-repair configuration and calibration that is increasingly essential to restore full functionality after physical repairs. GE's own training webinar materials highlight being able to "enter service mode" and "run calibration routines" along with targeted tests of fans, heaters, and sensors.[45] In refrigerators, industry reporting has described cases where replacing an ice maker or other component requires reprogramming and calibrating tolerances via Smart HQ. As of 2025, GE has advertised a subscription to the Smart HQ service at $600.00 per year (USD) in addition to a $199.00 (USD) Bluetooth service module.

The Smart HQ service illustrates how modern repair practices frequently involve software-based diagnostic tools for component actuation and calibration routines. Without this software layer, technicians may leave physically repaired devices out of spec. Though GE markets these tools as ways to reduce misdiagnosis and accuracy of repair, it is indicative of a broader trend of relying on software tools to gatekeep access to repair, limiting participation to professional repairers or those willing to invest in commercial grade subscriptions to software platforms.[46]

In sum, the foregoing examples underline the notion that repairing modern products and devices using only analog or physical tools is increasingly becoming a thing of the past. The decisive tool in many situations is often a software-layer, whether through accessing on-board software using special keys or codes or with software-enabled supplementary tools. These can be required in either identifying fault states, authenticating replacement parts as 'genuine', or calibration routines as the final step.

3. Right to Repair Mandates Requiring Access to Software

Given the crucial and instrumental role of software tools in repair practices, it should come as no surprise that access to these resources forms a key component of R2R legislative frameworks in both the United States and the EU. The following sections survey a selection of recent R2R policy developments in both jurisdictions that impose obligations on manufacturers to provide software tools.

3.1 The European Union's R2R Framework

To provide a brief introduction to lawmaking in the EU, its legislative institutions operate under the principal of conferral. This means that it may only act within the competencies stipulated by its constating treaties. The two primary legislative instruments created by EU institutions are "Regulations" and "Directives". The former has general application and are binding in their entirety, making them directly applicable in all EU member states. Directives, on the other hand, are binding as to the result to be achieved, leaving member states the choice of form and methods and requiring transposition into national law by a prescribed deadline.

In practice, Regulations are used for uniform and immediately operative rules, while Directives set common objectives and minimum standards that national legislatures must implement. A core legislative competency of EU institutions is a focus on internal single market harmonisation and product standardisation.[47] As is described further below, this legislative focus helps lay the groundwork for a robust and prescriptive R2R framework in the EU, including mandated access to software and software-based tools.

The EU has embarked on a broad and ambitious R2R agenda as part of its sustainability and circular economy goals. Launched under the European Green Deal in 2019 and the Circular Economy Action Plan (CEAP) in 2020, this agenda aims to extend product lifespans, reduce e-waste, and empower consumers and independent technicians to repair products rather than replace them. A key focus of the EU's R2R policy has been in ensuring access to the parts, information, and software-based tools needed for repair.

Over the past five or so years, the EU has introduced a comprehensive suite of laws and policies that contribute to its R2R framework, including a mixture of high-level strategic initiatives that provide direction, new legislation on product design, and consumer protection laws to promote repair and transparency:

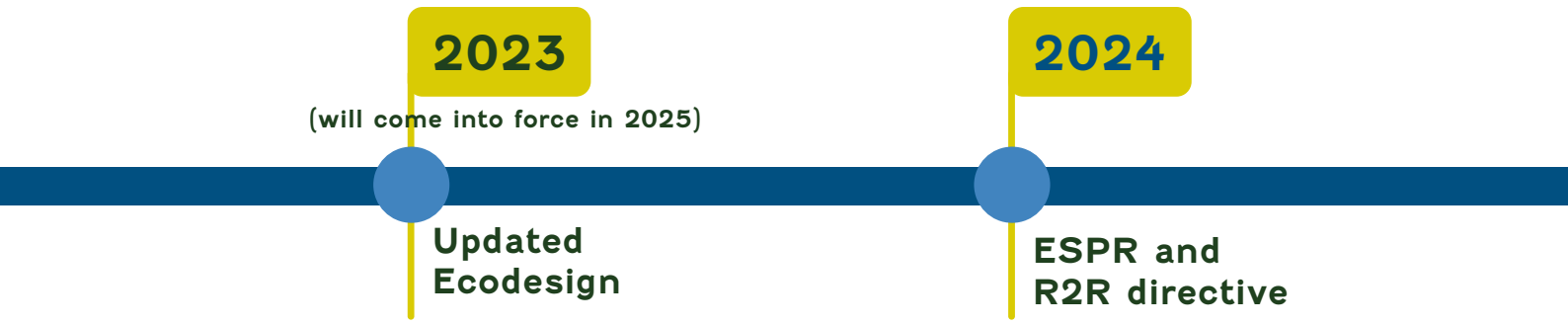
3.1.1. Ecodesign for Sustainable Products Regulation

The ESPR[48] creates a framework for setting product design and performance requirements and supersedes the older (2009) Ecodesign Directive.[49] It entered into force on 18 July 2024 and empowers the European Commission to adopt delegated acts imposing specific sustainability and circularity requirements on nearly all categories of physical goods, including software-dependent devices. These requirements cover aspects like durability, repairability, and recyclability and information disclosure at the time of sale. Crucially, the ESPR mandates the development of Digital Product Passports (DPP) for certain products. These are digital records that provide standardised information on a product's composition and repairability (including the availability of spare parts, software tools, and instructions) to consumers, repairers and other stakeholders.

The ESPR can be best understood as setting the EU's "design for repair" agenda, ensuring new products are engineered with repair in mind and that information and resources (including software) is accessible via DPPs. Though the ESPR does not directly mandate disclosure or access to software necessary for repairs, Annex I of the proposal lists parameters to improve repair and maintenance, including "conditions for access or use of required hardware and software" needed to repair products.[50] Furthermore, future Ecodesign implementing rules may also require manufacturers to supply any specialised software or digital tools necessary to repair products.

3.1.2. The EU R2R Directive

Entering into force on 30 July 2024, the R2R Directive creates a unified EU framework to strengthen consumer rights and obligations of manufacturers. In contrast to the ESPR's focus on pre-market repairability by design, the R2R Directive sets the conditions for repair after a product has been purchased by a consumer. The aim of the R2R Directive is to make repair a more attractive and accessible option throughout the product's useful life. It amends a number of existing legal instruments (such as the Sale of Goods



Directive) to establish a suite of new standardised obligations on manufacturers of certain product types. The deadline for EU member states to implement the R2R Directive is 31 July 2026.

Touching upon software tools specifically, the R2R Directive's Annex II provides a list of product categories for which manufacturers must provide parts and "tools" needed for repair at a "reasonable price".[51] In this context, "tools" are defined broadly to encompass not only physical tools, but also repair-related software tools, firmware, diagnostics, or similar auxiliary means needed to carry out repairs properly. Recital 18 of the Directive clarifies that:

"...[M]anufacturers are to provide access to spare parts, repair and maintenance information or any repair related software tools, firmware or similar auxiliary means."

This general principle is reflected at Article 5(6) of the R2R Directive, which sets out the general obligations on manufacturers to facilitate the R2R for certain goods and products[52], including that:

> *"Manufacturers shall not use any contractual clauses, hardware or software techniques that impede the repair of goods...unless justified by legitimate and objective factors including the protection of intellectual property rights..."*

Put together, these obligations imply that, where manufacturers of pre-existing software-dependent devices have invoked techniques that necessitate software tools for effective repair, they must now provide access to those tools and utilities as part of their obligations under the Directive. Looking ahead, this also means that device manufacturers may not employ software restrictions or keys on future products purely to block independent repairs.

3.1.3. EcoDesign Regulation for Smartphones and Tablets (ERST)

Acting parallel to the ESPR, the EU enacted the ERST[53] in 2023 under the old 2009 EcoDesign Directive. These rules came into effect on 20 June 2025 and are intended to ensure that mobile phones and tablets (in particular) sold in the EU are repairable. The ERST imposes a number of new and detailed obligations on device manufacturers in relation to software and software tools, including that manufacturers supply firmware, diagnostic software, or digital keys needed in repair activities. These are the first binding set of prescriptive and detailed rules creating the R2R smartphones and tablets in Europe.

The ERST implicitly distinguishes between manufacturers' obligations to release operating system updates and software tools needed for "serialised parts", or parts

that are subject to parts-pairing techniques. 'Serialised parts' are defined as:

"...a part which has a unique code that is paired to an individual unit of a device and whose replacement by a spare part requires the pairing of that spare part to the device by means of a software code to ensure full functionality of the spare part and the device".

In the case of smartphones, for example, the ERST repeats language found in the R2R Directive by requiring manufacturers to:

> *"...provide non-discriminatory access for professional repairers and end-users to any software tools, firmware or similar auxiliary means needed to ensure the full functionality of those spare parts and of the device in which spare parts are installed during and after the replacement..."*

Being enacted pursuant to the 2009 EcoDesign Directive, an important feature of the ERST is that EU member states are empowered to "designate authorities responsible for market surveillance" to ensure compliance with these requirements. This entitles regulatory authorities at the member state level to:

> *"...organise appropriate checks on product compliance...and oblige the manufacturer or its authorised representative to recall non-compliant products from the market... [and] require the parties concerned to provide all necessary information, as specified in the implementing measures [and] take samples of products and subject them to compliance checks."*

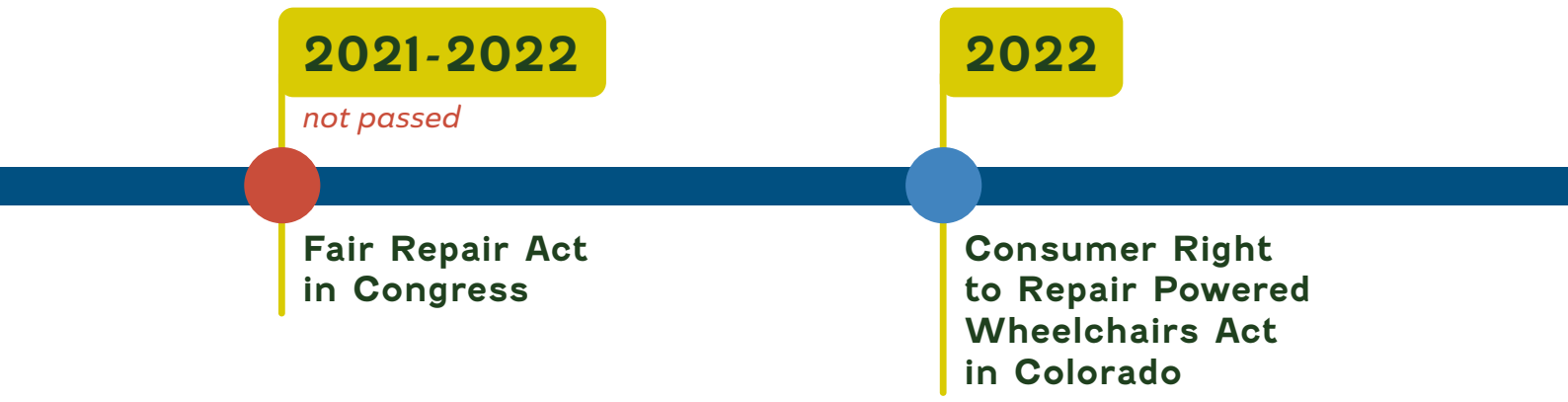
Member states could therefore launch compliance investigations under the ERST that require device manufacturers to provide access to various software tools and firmware, as w ell as engage in reverse engineering investigations to determine regulatory compliance. As is discussed further in Part 4 below, this has important implications for FTA source code protections in some recent trade agreements.

Each of the above policy frameworks contributes to the EU's increasingly comprehensive policy architecture for the R2R. The ESPR (and product-specific regulations pursuant to it) addresses the supply side of product design and produce obligations to supply parts, software, and information. The R2R Directive, on the other hand, addresses the demand side, including emboldened consumer rights, transparency, and fostering aftermarket repair services. These measures mutually reinforce one another to create a layered approach to the R2R throughout the EU.

3.2 R2R Legislation in the United States

In contrast to the EU's more centralised approach, the United States has seen R2R initiatives emerge primarily at the state level. To date, there is no federal R2R statute, though a proposed "Fair Repair Act" was introduced and discussed in Congress in 2021-2022 but never passed.[54] Nevertheless, advocacy continues in Washington, and federal agencies like the Federal Trade Commission (FTC) have shown interest in addressing restrictive repair practices through anti-trust enforcement.[55] In the meantime, state legislatures have led the charge, being primarily responsible for consumer law. As of early 2025, lawmakers in all 50 states have introduced or passed some form of R2R legislation.[56]

Being legislated at the state level, these statutes only regulate conduct occurring within the territory of those states that have enacted them, such as the sale or service of goods to residents in that state. This means that a resident of a state without R2R legislation cannot "import" another state's R2R protections simply by travelling there or owning a product sold in a state with R2R legislation in effect. Despite their territorial limitations in this regard, state-level R2R bills in the United States have made enormous progress in creating new obligations on manufacturers to provide parts, tools, information, and software to support independent and self-repair. Below is an analysis of a subset of these state level R2R laws that emphasise the provision of access to software or software-enabled tools as an illustration of the U.S. approach.



3.2.1. New York's Digital Fair Repair Act (2023)

New York was the first U.S. state to pass a broad-based consumer electronics R2R law. ***The Digital Fair Repair Act,*** which came into force in late 2023, requires electronics manufacturers to make available to owners and independent repair providers "the parts, tools, and documentation" for most devices first manufactured or sold in New York.[57] In practice, this means that original equipment manufacturers (OEMs) must provide (either directly or through authorised repair partners) documentation, parts, and tools.

The underlying 'fairness' principle that shapes the bill is that manufacturers must provide these resources to independent and third-party technicians on the same terms that their own 'authorised' service providers receive them. Importantly, the New York bill explicitly defines "tools" to include:

> *"...any software program, hardware implement, or other apparatus used for diagnosis, maintenance, or repair...including software or other mechanisms, that provide, program, pair a part, calibrate functionality, or perform any other function required to repair or update the original equipment or part back to fully functional condition..."*

While New York's Act establishes quite broad obligations in this regard, it also contains an important limitation to protect intellectual property, making clear that nothing in the bill requires a manufacturer to "divulge any trade secret or licence any intellectual property".

In terms of practical scope, New York's Fair Repair Act covers "digital electronic equipment", which is broadly defined as any product that depends on embedded digital electronics to function. At the same time, the bill also excludes many categories of equipment, including motor vehicles, off-road equipment, medical devices, home appliances, gaming consoles, and certain industrial and commercial equipment. The effect is that New York's law is limited to consumer-grade electronics, smartphones, and similar personal devices, while at the same time imposing quite broad and far-reaching obligations on manufacturers of those products. In spite of these important carve-outs, New York's ***Digital Fair Repair Act*** is generally viewed among R2R advocates as a landmark in requiring manufacturers to share both physical and software-based tools needed for independent repairs.

2023

New York's Digital Fair Repair Act

Consumer Right to Repair Agricultural Equipment Act in Colorado

2024

Minnesota's Digital Fair Repair Act

as of 2025 State level legislation on R2R introduced in all 50 States

3.2.2. Minnesota's Digital Fair Repair Act (2024)

Following New York's lead, Minnesota began charting a path toward its own Digital Fair Repair Act in 2023, coming into effect on 1 July 2024.[58] This bill is considered one of the broadest state-level R2R bills to date, covering a wide range of electronic products that fall under the umbrella of "digital electronic equipment". This is defined as:

> *"...any hardware product that depends, in whole or in part, on digital electronics embedded in or attached to the product in order for the product to function..."*

Similar to the New York bill, however, Minnesota's act exempts certain products and devices, including motor vehicles, medical devices, video game consoles, and off-road heavy equipment.[59] Despite these exclusions, Minnesota's law essentially covers everything else in the consumer and business electronics realm.[60] One consequence of this expansive approach (contrasting from New York's bill) is that the Minnesota bill applies to home appliances like washing machines, smart thermostats, and even 'enterprise computing systems' (in offices and commercial settings). Like New York's bill, Minnesota's includes a carve-out for intellectual property, clarifying that no trade secrets need to be shared by manufacturers. In sum, Minnesota's bill fills some of the loopholes that were watered down with New York's law and firmly establishes that software support and software-based tools are not a legal expectation in that state.

3.2.3. Other State R2R Laws Requiring Software Access Access

Beyond New York and Minnesota's general electronics statutes, several other U.S. states have pursued more specialised R2R laws that explicitly mandate access to software or firmware as part of necessary repair resources:

Colorado has been an early mover on niche R2R issues with the nation's first R2R law for medical mobility devices in 2022, the Consumer Right to Repair Powered Wheelchairs Act.[61] Effective 1 January 2023, the law requires a wheelchair manufacturer to provide owners and independent technicians with parts, tools, documentation, and "embedded software" needed to repair a powered (electric) wheelchair. The Act defines "embedded software" as:

> *"(a) means programmable instructions provided on firmware d elivered w ith an electronic component of equipment or with any part for the purpose of restoring or improving operation of the equipment or part; and*
>
> *(b) includes all relevant patches and fixes that the manufacturer makes to equipment or to any part for the purpose of restoring or improving the equipment or part."*

The Act also defines tools as including "any software program...that provides, programs, or pairs a new part... or calibrates

functionality." Similar to the New York and Minnesota laws, Colorado's Act also stipulates that manufacturers do not have to divulge trade secrets as part of their obligations to provide these resources.

Building on this success, Colorado also enacted the Consumer Right to Repair Agricultural Equipment Act in 2023, the country's first R2R law covering farm machinery specifically.[62] Starting 1 January 2024, agricultural equipment manufacturers in Colorado must supply to farmers and independent mechanics the resources needed to repair their equipment. Those resources are defined to include "any documentation, parts, embedded software, firmware, tools... or data". The bill is unique in its approach to include "data" in the list of items that must be provided by manufacturers, including any machine-generated performance or diagnostic data needed for repairs. In essence, Colorado's agricultural R2R bill ensures that farmers have access to the same diagnostic software and firmware tools that dealers have, directly addressing software barriers and firmware restrictions that have plagued tractor and combine repairs in recent years.

Several other U.S. state laws have targeted specific product areas with R2R provisions that involve software access. This includes Massachusetts' longstanding automotive bills and the disclosure of 'vehicle data'[63], and California's Right to Repair Act (Senate Bill 244)[64] that addresses consumer electronics, which provide less explicit references to things like firmware, calibration programs, or other software-based tools. The overall trend reflects a growing consensus among state-level lawmakers that modern products and devices absolutely require access to firmware, software diagnostics, and digital keys and that these resources form an essential part of R2R legal frameworks.

Together, both the United States and EU approaches to the R2R demonstrate a converging understanding (despite somewhat distinct orientations). They both make clear that access to embedded software and software-based tools is essential to enable independent repair.

In both cases, manufacturers are being told that providing physical parts or components and written instructions is not sufficient. Concrete obligations to transfer or provide access to these software tools are increasingly a core component of R2R legal frameworks on both sides of the Atlantic.

4. Source Code Protections in Trade Agreements

4.1 Background & Context

Recent bilateral and plurilateral FTAs have included "e-Commerce" or "Digital Trade" chapters that restrict governments from requiring transfer or access to "source code" as a condition for market access.[65] Given the essential role of software and software-based tools, this creates a potential overarching transnational legal barrier to the successful implementation of R2R mandates at the domestic level in both the U.S. and EU. This is because FTAs are binding international treaties, and as a result, states are obligated under international law to ensure their domestic measures conform to those commitments. Therefore, where domestic laws (such as R2R statutes) conflict with FTA obligations, they create a risk of non-compliance with international commitments that could lead to disputes under the agreement and, ultimately, result in trade sanctions. Because of this, the risk of inconsistency with FTA commitments often results in national governments or legislators amending or interpreting domestic laws to avoid breaching their obligations under FTAs, or to bring measures into conformity once they have been challenged through dispute settlement.

The precise wording and implications of special source code protections vary between FTA texts, but the first clear template for these rules is found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP is a large plurilateral FTA in which neither the U.S. nor the EU are parties, but which nevertheless establishes a model that has been followed by both entities in subsequent agreements. Article 14.17 of the CPTPP stipulates that:

> *"No party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory"*

The ban on mandated transfer or access means that governments arguably cannot impose requirements on manufacturers of devices with embedded software to transfer or provide access to that software. This presents a significant obstacle for the proper operation of R2R laws. And though FTA source code protections occasionally include narrow exceptions (for example, to allow manufacturers to modify source code to comply with domestic legislation, or disclosure in the context of a judicial proceeding), the default rule is non-disclosure.[66]

4.2 Distinctions Between Source Code and Object Code

To understand the potential scope and implications of FTA source code protections it is worth briefly outlining the technical and terminological distinctions between "software", "source code", and related concepts. At a very basic level, "source code" is a representation of a computer program in human readable language.[67] It is normally the version of software as originally written by its author. For example, if a user right clicks on a webpage and selects "view page source", what is displayed serves as an instructive example of source code and its role in programming.

This can be distinguished from object code, which is produced when source code is translated (or "compiled") into machine-readable language understandable by a computer (i.e., ones and zeroes).[68] Source code is generally written at a high level of abstraction and therefore agnostic to the end-computing platform or hardware that it will be executed on. In contrast, object code must be tailored to a particular computer, system, virtual environment, or platform on which it is executed.

Viewed in this way, source code is analogous to the architectural blueprints of a building, detailing its design, materials, and functionality. Object code, on the other hand, reflects the building's physical components assembled into a tangible whole. It is for this reason that access to source code confers a whole host of capabilities on those who have access to it, including secondary activities and discoveries such as bug detection, error correction, modification, and enhancements.

4.3 Analysis of Key Agreements and Provisions

FTA source code protections have found their way into numerous agreements since their first intimation on the CPTPP. Some agreements have expanded on the potential scope of subject-matter that may be covered by these prohibitions, while others have included clarifying language that may help narrow their application in certain cases, including R2R policies.

4.3.1. United States-Mexico-Canada Agreement (USMCA)

Serving as an example of the more expansive approach is the United States-Mexico-Canada (USMCA) agreement, which at Article 19.16 provides that:

> *"No party shall require the transfer of, or access to, a source code of software owned by a person of another Party, **or to an algorithm expressed in that source code,** as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory."*

In invoking this language, the USMCA expands upon the CPTPP approach by including "algorithm" in the subject-matter shielded from transfer or access. The USMCA's Article 19.1 defines "algorithm" as:

> *"...a defined sequence of steps, taken to solve a problem or obtain a result."*

This broad definition has some important implications for R2R policy. On the one hand, requiring access to a compiled binary (object code) in the form of repair software or an access key to address parts-pairing is not the same as providing source code. On this basis, one line of argumentation may be that software and software-based tools necessary for repair are not captured by the FTA prohibition against disclosure or access. But on the other hand, the expansion of the prohibition to 'algorithms expressed in source code' leaves open the possibility for arguments from manufacturers that the use of access keys or repair software reveals aspects of the underlying algorithms or 'software logic', broadly construed. This line of argumentation could be used to support a more restrictive interpretation of the FTA language by manufacturers, industry groups, or government lawyers litigating trade cases that, in effect, limits access to software and software-based tools needed for repair even when they are distributed in object code.

Importantly, the USMCA also includes an important exception for investigations and inspections. Subsection (2) of Article 19.16 provides that:

> *"This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding..."*

An important qualifier in this exception is the word "specific", which requires that a regulatory or judicial investigation be ad-hoc or outside of a general regulatory scheme to escape the FTA's general prohibition on disclosure or access. This has potentially important implications for R2R legislation such as those under the EU's ERST that envision "compliance checks" and market surveillance measures. Thus, while a general exception permitting regulatory requirements to disclose or provide access to source code would be presumably beneficial for R2R frameworks, the limitation to 'specific' proceedings is likely to significantly narrow this potential.

The potential problems for the R2R created by USMCA's approach transcends the narrow scope its exceptions, however. The potential for conflict arises not only when R2R frameworks are enforced, but also when they are enacted.

Therefore, the legal requirement on manufacturers to provide software, access keys, or repair tools to third parties could itself be seen as "requiring access to a person of another Party's algorithms" regardless of whether enforcement or investigation of those obligations is carried out by a regulatory body.

4.3.2 EU-Japan Economic Partnership Agreement (EU-Japan EPA)[69]

The EU has also included source code provisions in its more recent trade deals, though with distinctly European nuances. The EU-Japan Economic Partnership Agreement (EU-Japan EPA) was one of the first EU FTAs to include such a rule. Notably, Article 8.73 similarly prohibits state parties from requiring transfer or access to source code while also including some important caveats. The EU-Japan EPA also does not confine its prohibition on source code access or transfer to processes necessary for import, distribution, or to otherwise gain market access. The absence of this contextual qualification in the EU-Japan EPA broadens the scope and application of source code protection. On this basis, it may give product manufacturers greater justification for arguing that domestic R2R mandates requiring software disclosure inherently conflict with the terms of the agreement.

In contrast to the USMCA, the EU-Japan EPA includes a more robust set of exceptions that would permit disclosure or access to source code, including those for "commercially negotiated contracts" and for the purposes of "public procurement". But on the other hand, the EU-Japan EPA includes clarifying language that may also broaden the practical scope of what is included as "source code":

> *"For greater certainty, 'source code of software owned by a person of the other Party' includes source code of software contained in a product."*

While there is no available evidence of manufacturers relying upon this clarification to thwart the operation of R2R laws, the expansion to source code 'contained in a product' leaves open the possibility for argument by manufacturers that obliged sharing of firmware or diagnostic tools with third parties is the same as sharing the code in that product. As is the case with the USMCA's expansive notion of 'algorithm', the risk with the EU-Japan Agreement's embrace of source code in products lies in the consequences of its interpretation. And given that finished products are ordinarily sold and shipped with only object code (binaries), this could result in manufacturers arguing, in effect, that these rules extend to software tools in object code form as well. This could have important implications for devices such as the GE Smart HQ service calibration tool and the Taylor C602 soft-serve ice cream machine discussed in Part 2.

4.3.3 EU-Singapore Digital Trade Agreement (EU-Singapore DTA)[70]

In May of 2025, the EU and Singapore signed a standalone Digital Trade Agreement ("EU-Singapore DTA"), the first such digital-only agreement for the EU. This agreement follows the template of EU's recent FTAs but is focused exclusively on digital trade issues. It contains the familiar source code provision, but with some important exceptions. Crucially, it includes a similar exception to the USMCA's regulatory or judicial investigation, but with much more permissive language:

> *"[This Article] does not affect the right of regulatory, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws or regulations that are not inconsistent with this Agreement"*[71]

The DTA goes on to provide further carveouts and clarifications for "regulatory assessment bodies" at Article 11(3)(a):

> *"[Nothing in this Article shall affect] ... the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies of a Party to require transfer of, or access to, source code of software, either prior to or following import, export, distribution...to secure compliance with its laws or regulations pursuing legitimate public policy objectives..."*

Importantly, the carveouts for regulatory assessment bodies allow both "transfer" and "access" to source code, presumably permitting regulators to share or distribute it to third parties. In a clarifying footnote, the Agreement defines "conformity assessment body" as referring to "a relevant government body or authority of a Party...carrying out the procedures of assessment of conformity with applicable laws or regulations of that Party."

Upon a cursory reading, the EU-Singapore DTA appears to be far more permissive than the USMCA in allowing for regulators to require disclosure or access to source code beyond specific investigations or judicial proceedings. It also cedes some ground to "laws or regulations pursuing legitimate public policy objectives" and permits source code access and transfer to "secure compliance with its laws or regulations". The flexibility offered to domestic priorities and objectives seems to point in the general direction of R2R frameworks.

Pouring some cold water on this optimism, however, the conflict persists because of how domestic R2R frameworks are operationalised in practice. In general, R2R frameworks operate as broad, horizontal consumer rights regimes. They apply to all consumers and businesses rather than to discrete enforcement or compliance functions of governments or state bodies.

As such, even though the EU-Singapore DTA exceptions evoke greater flexibility, the continuous and universal character of R2R frameworks would likely fall outside of the

narrow, ad-hoc enforcement context contemplated by this more permissive exception framework. In practice, therefore, this means that despite its more flexible wording, the exception is unlikely to shield comprehensive R2R legislation from conflict with the underlying FTA prohibition on source-code disclosure.

4.3.4 Development of Policy Positions

The above demonstrates a clear trend toward incorporating source code protection clauses into FTAs among advanced economies.[72] Furthermore, parallel to these bilateral and regional FTAs, dozens of countries have also attempted to craft multilateral digital trade rules through the World Trade Organization. In 2019, a large coalition of WTO members launched the Joint Statement Initiative (JSI) on Electronic Commerce, aiming to negotiate global disciplines on e-commerce and digital trade.[73] By 2023, JSI talks had attracted over 90 economies (including major players like the EU, US, Japan, and China).

The larger policy shift and turning point in these trends came in late 2023 when the United States made a surprise policy reversal that fundamentally shifted the JSI dynamics. USTR Katherine Tai withdrew several U.S. proposals that had been on the table since 2019, including the rules requiring unrestricted data glows and prohibiting mandated access to source code.[74] Essentially, Washington dropped its longstanding demands for binding WTO commitments on free data movement and source code protections. The USTR's statement on this point was brief, stating that:

> *"Many countries, including the United States, are examining their approaches to data and source code, and the impact of trade rules in these areas. In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those domestic policy considerations..."*

Core to these 'domestic policy considerations' have been addressing anti-competitive activity in the digital economy, including issues like the R2R.[75] In a letter thanking President Biden for the USTR's reversal on digital trade, a group of senators and house representatives noted that source code and algorithm secrecy risked gutting "right-to-repair laws being enacted in states nationwide", urging keeping policy space for domestic tech regulation.[76] At present, the U.S. position on digital trade (and FTA source code protections in particular) remains in the process of recalibration, and this pivot from its initial leadership role acknowledges the need to reevaluate the potential impact of these rules. Indeed, if domestic R2R frameworks are to fulfil their normative and operational goals, overarching trade commitments cannot pre-empt clear obligations on manufacturers to provide reasonable access to software and software-based tools.

The EU, for its part, has been actively advancing its own digital trade agenda; albeit with a somewhat distinct philosophy from the United States. Though the EU had historically been more hesitant than the U.S. to embrace sweeping e-commerce provisions (given its commitment to privacy and confidentiality)[77], it has since more fully championed digital trade chapters. The EU is motivated (in part) by the need to ensure secure strong consumer protections in the digital environment, reflecting its inclination toward broad-based regulation of technology firms. This is codified in the European Commission's 2021 trade strategy, which makes supporting Europe's "digital agenda" a priority for trade policy.[78] As a result, contemporary EU trade agreements such as the EU-Singapore agreement commonly contain self-standing chapters on digital trade, with source code protections permitting regulatory oversight included.

In looking at the larger and international picture that results from these trends, the outcome on source code provisions remains uncertain, but there is room for optimism.[79]

As a positive development, the JSI's final slimmed-down agreement now excludes the controversial source code clause.[80] At the same time, the fact that a sizable group of WTO members were willing to negotiate such rules prior to the U.S. reversal evidence broader international interest in source code protections, at least to some extent. It is therefore conceivable that outside the WTO, smaller plurilateral agreements will carry forward some iteration of these rules (for example, as part of expansion of the CPTPP membership). Furthermore, there remains the possibility for new alliances of the willing, with groups of countries that may agree on broader digital economy pacts under the OECD framework or as standalone treaties.

On the other hand, much has changed since the first iteration of FTA source code protections were introduced as part of the CPTPP and reformulated as part of the USMCA. The burgeoning growth of the R2R movement and economic circularity have given policymakers reason to stop and rethink many of their economic and industrial policies since the COVID-19 pandemic. Furthermore, the growing interest and concern in algorithmic governance and the societal impacts of persuasive technologies and platforms lean heavily toward greater scepticism of these rules as we move into the future. Taking an even larger view, shifting geopolitical dynamics are increasingly requiring countries to pursue protectionist strategies relating to their markets and national security. Each of these factors suggests that national lawmakers and trade negotiators will assess FTA source code protections with greater scrutiny in the months and years ahead.

5. Outstanding Issues & Ambiguities

When analysing the source code protection language in recent FTAs in light of domestic R2R frameworks in the United States and the EU, there are a number of uncertainties and ambiguities that become apparent:

Do R2R frameworks require transfer or access to "source code"?

R2R frameworks on both sides of the Atlantic are generally agnostic to whether software or software-based tools must be distributed in object code or source code form. In many cases, such as New York's Digital Fair Repair Act, legislation expressly excludes any obligation that would result in the disclosure of trade secrets. This suggests that manufacturers are not expected to share source code. Nevertheless, when FTAs refer only to "source code of software" without mentioning "algorithms" or "software contained in products", a baseline interpretive risk remains.

The act of requiring manufacturers to provide diagnostic software, firmware updates, or calibration programs could be construed as requiring "access to source code"

insofar as these software-based tools are intimately connected to, and often derived from, the manufacturer's proprietary code.

That risk is materially amplified where FTA language extends beyond source code itself to cover "algorithms" or "software contained in products", such as in the USMCA and the EU-Japan agreements. These formulations expand the protected subject matter from human-readable code to the functional logic of software and its embedded implementations. This increases the likelihood that repair software or access keys (typically distributed in object form) could be characterised as falling within the scope of the prohibition. **In such cases, the FTA's non-disclosure rule could more readily be invoked to pre-empt domestic R2R laws that require manufacturers to provide software-based repair tools, even when no access to source code per se is sought.**

Pre-emption of domestic law

As addressed in Part 4 above, trade agreements are binding on states and their governments, but they do not automatically invalidate domestic laws in the way a national constitutional court might. Instead, enforcement occurs through state-to-state dispute mechanisms. This means that a government can be held internationally responsible for breaching its treaty obligations, but the domestic R2R statute remains formally in force unless the state chooses to amend or repeal it. For this reason, FTAs with restrictive source code protections are unlikely to directly strike down domestic R2R legislation.

However, a state found in violation could face international dispute-settlement proceedings, either under an FTA's own mechanism or at the WTO. This could lead to retaliation, compensation claims, or negotiated settlements. In practice, the prospect of such proceedings (or persistent complaints from trade partners) can exert strong diplomatic and economic pressure on governments to narrow or revise their R2R rules to ensure conformity. This indirect but potent form of pre-emption may, over time, lead to the softening or erosion of R2R frameworks at the U.S. state level or to narrower interpretations of EU Directives and Regulations to avoid potential trade conflicts.

Beyond pressures applied once R2R frameworks come into force, pre-enactment trade law compliance also could play a significant role in shaping future laws. Within the EU, legislative and regulatory bodies often vet new policy proposals to ensure their compatibility with existing trade commitments. This can lead to the dilution or narrowing of initial R2R ambitions. For example, during the drafting of the EU Artificial Intelligence Act, the EU Commission's Directorate-General for Trade reportedly urged the Directorate General JUST to limit provisions allowing regulators to access source code because of the EU's commitments under the EU-UK Trade and Cooperation Agreement.[81]

This type of international coordination illustrates that trade law obligations can constrain domestic policy design ex ante, even before any international dispute arises.

Exceptions for regulatory bodies, proceedings, and investigations

Many of the FTAs surveyed above include exceptions that allow some form of transfer or access to source code for particular public-interest purposes, regulatory processes, and other procedures. These exceptions vary significantly in their scope and potential application to R2R frameworks. Where R2R legislation imposes general obligations on manufacturers to provide access to software and software-based tools, it is not clear that these measures would be captured by the general exceptions for "regulatory assessment bodies". This is because statutory obligations on manufacturers that are enforced through private litigation are not "regulatory" in a strict sense. On the other hand, where R2R frameworks include oversight by administrative authorities to ensure compliance and enforcement with these standards, they are more likely to be saved by the exemptions found in various FTAs.

In practice, however, these exceptions are difficult for domestic regulators to operationalise. Triggering them would normally require an authority to issue a formal request for information or access to source code in connection with a specific investigation or compliance verification. Yet, most domestic regulators responsible for R2R frameworks and consumer protection are neither mandated nor resourced to invoke trade-law exceptions in the first place. They may also be unaware of this possibility entirely. Therefore, even where FTAs may be interpreted to technically permit source code access or disclosure for specific regulatory purposes related to the R2R, these clauses are unlikely to be an effective solution for broad-based, horizontal R2R consumer frameworks.

6. Weighing the Potential Paths Forward

1 Amendments to Domestic R2R Frameworks

One approach to resolving potential conflicts and ambiguities may be to amend domestic R2R frameworks to include clarifying provisions. This could, for instance, involve interpretive clarifications that obligations on manufacturers to provide software or software-based tools does not imply the obligation to divulge "source code" or "algorithms" in contravention of any trade agreement. This would fall short of a satisfactory resolution, however, for at least three reasons. The first is that this would come at the cost of potentially weakening the scope of R2R legislation's application to certain software-based tools that the manufacturer asserts constitute 'source code'. In other words, this would leave manufacturers largely in charge of deciding which tools are subject to R2R regulation and which are not. Secondly, this approach would fail to resolve the definitional and conceptual ambiguities that are present across various FTAs, including the application of exemptions for public interest regulatory processes and related investigations. Finally, the process of amending numerous domestic R2R laws substantially increases the likelihood of disharmonisation while providing the opportunity for industry lobbying to weaken the effectiveness of these laws over the long term.

2 Relying on Existing Public Interest Exemptions in FTAs

Domestic lawmakers and R2R advocates may alternatively set their sights on the existing exemptions in FTAs for public interest regulatory oversight and formulate arguments that R2R frameworks fall within their scope. While some agreements contain exemptions that could apply to certain approaches to R2R policy, there is significant deviation. For example, the EU-New Zealand agreement permits only "access" to source code as part of regulatory exemptions, whereas the EU-Singapore DTA permits both "transfer" and "access". This distinction is essential, because the proper

operation of R2R policy involves manufacturers sharing and distributing software and software-based tools to consumers and independent repairers (third parties). This necessarily requires more than regulatory bodies 'accessing' source code, but also widespread disclosure and provision for the benefit of others. This lack of uniformity results in the existing exemptions in FTA frameworks being inadequate for R2R policy. They are neither consistent enough to cover the various approaches to R2R policy nor broad enough to address the need to share software and software-tools with the public and third-party repairers.

Recalibrating Trade Policy to Support the R2R

Likely the most productive and effective approach to resolving these tensions is to advocate for a recalibration of digital trade policy to abandon source code protections entirely. Even beyond the R2R, the potential societal and democratic risks of preventing access and transfer to source code is simply too high. Where algorithmic and software-enabled products and services are having an increased impact on social and democratic processes, trade negotiators should not be tying the hands of national lawmakers to craft policy that safeguards the public interest and national security. Similar to the R2R, this will inevitably require access to source code.

If FTA source code protections are to remain, specific carveouts are needed for R2R frameworks given that they operate as much more than mere compliance and enforcement schemes. Providing room for optimism in this latter strategy is the EU's willingness to include increasingly permissive exemptions in recent FTAs[82] along with the United States' reversal and re-evaluation of its broader approach to digital trade. The structure and approach to these exceptions must be significantly broadened, however, if the R2R is to be embraced by them in future deals.

At present, the United States is in the process of renegotiating the USMCA and reevaluating a large number of its trade relationships around the world. This presents an opportunity to craft a new approach to digital trade that either removes prohibitions on source code disclosure entirely or includes a clause carving out the sharing of software and software-based tools for legitimate repair, safety, or environmental purposes. Though no FTA at present currently includes a R2R-specific carveout in relation to digital trade and source code, future texts could be crafted with exceptions for the "maintenance of products" and the "safety of consumers" that shelter R2R laws and allow mandated access and transfer to software and source code beyond isolated investigations or as part of broader regulatory schemes.

7. Conclusion

The global proliferation of FTA source code protections has created a new and underappreciated layer of complexity for the R2R. Domestic laws in the EU and the United States now mandate access to software and software-based tools that are essential for repair. At the same time, digital trade agreements often define protected source code in such a way that can be interpreted to insulate these tools from disclosure to third parties. These competing regulatory currents appear to be on a collision course.

The report shows that although R2R laws do not generally demand source code explicitly, their obligations to provide firmware, calibration software, diagnostic applications, and digital keys can be positioned by manufacturers as encroaching on trade secrecy protection that is now enshrined in many FTAs. Ambiguous drafting (such as the inclusion of "algorithms" in the USMCA or clarifications about source code "contained in products" in the EU-Japan EPA) heightens the risk of overbroad interpretation. At the same time, international trade policy is undergoing a period of immense change. The United States has paused its promotion of rigid digital trade rules, opening space to consider new models, values, and priorities. The EU continues to export its digital trade agenda, but its agreements have increasingly incorporated exceptions that permit regulatory oversight and public interest measures. This convergence signals an opportunity for recalibration of digital trade and source code protections writ large.

Going forward, policymakers and trade representatives on both sides of the Atlantic should work to find links and points of common interest between digital trade rules and R2R mandates.

The most direct and effective approach would be to remove FTA source code protection clauses altogether.

Alternatively, explicit carve-outs for repair, maintenance, and consumer safety could reconcile these competing objectives as part of a broader ratcheting down of trade protections that impact software-related innovation. Without such adjustments, well-resourced manufacturers and lobbying efforts may leverage trade law to resist or dilute R2R obligations, thereby weakening the enormous hard-fought gains to environmental sustainability, consumer protection, and market competition.

In sum, the path forward requires better aligning trade and R2R policy. By modernising trade provisions to recognise repair as a legitimate public interest objective, and in recognising the crucial role of software and software-based tools, governments can safeguard both technological innovation and the ability for consumers and independent repairers to fix and maintain the products they own.

1 *As is explained in greater detail in Part 4, some recent agreements do not explicitly confine special protections against source code access or transfer to reviews or government processes that are conditional for market access. More recent EU agreements phrase the obligation more generally: "A Party may not require the transfer of, or access to, source code of software..." This could be interpreted much more broadly, and could mean that any law or regulation that seeks to obtain access or transfer of source code can be challenged as inconsistent with the FTA. See, Agreement between the European Union and Japan for an Economic Partnership (OJ L 330, 27 December 2018) art 8.73.*

2 *"Firmware" is a subset of software that is often embedded in hardware devices and provides low-level controls and direct hardware functionality. Users familiar with earlier iterations of Windows may recall updating "drivers" for various hardware peripherals like printers or scanners. Firmware plays a similar role in modern smart technologies and products. The distinction between software and firmware is therefore less technical than it is situational. Firmware refers to software that is devoted to performing a particular role, interacting closely with hardware to manage fundamental operations.*

4 *Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828, OJ L, 2024/1799, 10.7.2024*

5 *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for setting ecodesign requirements for sustainable products (the "ESPR") (amending Directive 2020/1828 and Regulation 2023/1542, and repealing Directive 2009/125/EC), OJ L, 2024/1781, 28.6.2024.*

6 *Commission Regulation (EU) 2023/1670 of 16 June 2023 laying down ecodesign requirements for smartphones, mobile phones other than smartphones, cordless phones and slate tablets, OJ L 214, 31.8.2023, p. 47.*

7 *Digital Fair Repair Act, N.Y. Gen. Bus. Law § 399-nn (enacted via Senate Bill S4104A / Assembly Bill A7006B) (signed December 28, 2022, effective December 28, 2023).*

8 *Digital Fair Repair Act, Minn. Stat. § 325E.72 (2023) (effective July 1, 2024).*

9 *Consumer Right to Repair Digital Electronic Equipment, Colorado HB 24-1121 (signed by Governor, expanding RT Repair statutes to include digital electronics).*

10 *For example, as early as the 1920s, industrial pioneer Henry Ford emphasised repairability as a design goal for Ford vehicles. See, Masayuki Hatta, "The Right to Repair, the Right to Tinker, and the Right to Innovate" (2020) 19 Annals of Business Administrative Science 143–157* **https://doi.org/10.7880/abas.0200604a** *accessed 6 July 2025..*

11 *One of the earliest legislative developments enshrining the Right to Repair in the United States was Massachusetts automotive right to repair bill, An Act protecting motor vehicle owners and small businesses in repairing motor vehicles, H.4362 (Mass, 187th Gen Ct, enacted 8 July 2012) (signed 8 July 2012).*

12 *Emma Bowman, "A new copyright rule lets McDonald's fix its own broken ice cream machines" (3 November 2024) NPR, online:* **https://www.npr.org/2024/11/02/g-s1-31893/mcdonalds-broken-ice-cream-machine-copyright-law,** *accessed 30 August 2025.*

13 *Ashley Belanger, "Trains were designed to break down after third-party repairs, hackers find" (13 December 2023) Ars Technica, online:* **https://arstechnica.com/tech-policy/2023/12/manufacturer-deliberately-bricked-trains-repaired-by-competitors-hackers-find/** *accessed 30 August 2025.*

14 *See, Anthony D Rosborough, "A Conceptual Map of the Right to Repair: Where Upcycling Fits In" in Peter Mezei & Heidi Härkönen, Research Handbook of Intellectual Property and Upcycling (Cambridge University Press, 2026) [Forthcoming].*

15 *European Parliament, 'New EU rules encouraging consumers to repair devices over replacing them' (Press Release, 21 November 2023)* **https://www.europarl.europa.eu/news/en/press-room/20231117IPR12211/new-eu-rules-encouraging-consumers-to-repair-devices-over-replacing-them** *accessed 28 August 2025.*

16 *See, for example, Minnesota's 2023 Digital Fair Repair Act (now Minn. Stat. § 325E.72), which requires OEMs to provide "documentation, parts, and tools, inclusive of any updates to ... embedded software" to owners and independent repairers, and (where a device has an electronic security lock) to provide the special documentation, tools, and parts needed to reset the lock, which may be supplied via a secure release system.*

17 *Kyle Wiggers, "New York's right-to-repair bill has major carve-outs for manufacturers" (3 January 2023) Tech Crunch, online:* **https://techcrunch.com/2023/01/03/new-yorks-right-to-repair-bill-has-major-carve-outs-for-manufacturers/** *accessed 3 September 2025.*

18 *Sam Metz, "Big tech and independent shops clash over 'right to repair' (30 March 2021) AP News, online:* **https://apnews.com/article/legislature-nevada-coronavirus-pandemic-laws-5ade405a7befdf16e9f0107b7e142be3**, *accessed 2 Sept 2025..*

19 *Examples include automakers' lawsuit against Massachusetts' vehicle data access law (Alliance for Automotive Innovation v Cambell) where the trade group sought to block the state's law expanding independent wireless access to telematics mechanical data on the grounds that is pre-empted national traffic and motor vehicle safety legislation. See, Dallin R Wilson, "Judge Denies Industry Challenge to Massachusetts Data Access Law" (11 February 2025) Sayfarth* **https://www.seyfarth.com/news-insights/judge-denies-industry-challenge-to-massachusetts-data-access-law.html**, *accessed 28 July 2025. Agricultural equipment manufacturer John Deere's Memorandum of Understanding with the National Farm Bureau is an example of where a voluntary agreement on the manufacturers' terms was sought to avoid prescriptive regulation that would have obliged the company to provide access to its proprietary software tools to farmers.*

20 *Michael Fridelwald & Oliver Raabe, "Ubiquitous computing: An overview of technology impacts" (2011) 28:2 Telematics and Informatics 55-65, 55..*

21 *Bruno Dorsemaine, Jean-Philippe Gaulier, Jean-Philippe Wary, Nizar Kheir and Pascal Urien, 'Internet of Things: A Definition and Taxonomy' (9-11 September 2015) in Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies 72–77 (IEEE) doi:10.1109/NGMAST.2015.71*

22 *IoT Business News, 'State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally' (IoT Business News, 4 September 2024)* **https://iotbusinessnews.com/2024/09/04/26399-state-of-iot-2024-number-of-connected-iot-devices-growing-13-to-18-8-billion-globally/** *accessed 6 July 2025.*

23 *See, Kyle Wiens, "You Gotta Fight For Your Right to Repair Your Car" (13 February 2014) The Atlantic, online:* **https://www.theatlantic.com/technology/archive/2014/02/you-gotta-fight-for-your-right-to-repair-your-car/283791/** *where the iFixit co-founder writes "You can't fix a computer with a wrench. Instead, fixing modern cars requires special diagnostic tools and official service information – information that some manufacturers don't share with independent repair techs.."*

24 *Maddie Stone, "Apple uses software to control how phones get fixed. Lawmakers are pushing back." (30 January 2024) Grist, online:* **https://grist.org/technology/apple-uses-software-to-control-where-phones-get-fixed-lawmakers-are-pushing-back/** *accessed 1 July 2025.*

25 *Gay Gordon-Byrne, 'Apple's War on Right to Repair Through Serial Numbers' (The Repair Association Blog, 25 September 2023)* **https://www.repair.org/blog/2023/9/25/apples-war-on-right-to-repair-through-serial-numbers** *accessed 13 September 2025.*

26 *Apple, "Apple to expand repair options with support for used genuine parts" (11 April 2024), online:* **https://www.apple.com/newsroom/2024/04/apple-to-expand-repair-options-with-support-for-used-genuine-parts/**, *accessed 5 July 2025.*

27 *Lauren Grenlee, "How Parts Pairing Kills Independent Repair" (17 January 2023) iFixit, online:* **https://www.ifixit.com/News/69320/how-parts-pairing-kills-independent-repair**, *accessed 1 July 2025.*

28 *Platform Security Summit, 'Guarding Against Physical Attacks: The Xbox One Story — Tony Chen, Microsoft' (YouTube, 21 October 2019)* **https://www.youtube.com/watch?v=U7VwtOrwceo** *accessed 12 September 2025.*

29 *Jean-Philippe Pomerleau, "VIN Lock: A Barrier to the Evolution of the Automotive Industry?" (15 January 2025) L'Automobile, online:* **https://www.lautomobile.ca/en/mechanics/vin-lock-a-barrier-to-the-evolution-of-the-automotive-industry** *accessed 2 September 2025.*

30 *"VIN locking" is related to the concept of "VIN burning", which is the practice of limiting a vehicle electronic control unit (ECU) or central computer to function with a single vehicle identification number or VIN. This allows the manufacturer to constrain the utility of a replacement part to work with only one particular vehicle. For a more fulsome explanation of these techniques, see Federal Trade Commission, Nixing the Fix: An FTC Report to Congress on Repair Restrictions (May 2021), 23* **https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf** *accessed 13 September 2025*

31 *For an up-to-date registry of operational and broken McDonald's ice cream machines, visit McBroken* **https://mcbroken.com/** *accessed 13 September 2025.*

32 *Andy Greenberg, "They Hacked McDonald's Ice Cream Machines – and Started a Cold War" (20 April 2021) Wired, online:* **https://www.wired.com/story/they-hacked-mcdonalds-ice-cream-makers-started-cold-war**, *accessed 20 August 2025.*

33 *Taylor Company, Model C602 Combination Shake/Soft Serve Freezer: Service Manual (Original Service Instructions 057888-S, January 2007; updated 14 July 2023)* **https://dslinc.com/wp-content/uploads/2024/12/C602.pdf** *accessed 13 September 2025.*

34 *Andy Greenberg, "The McDonald's ice Cream Machine Hacking Saga Has a New Twist" (23 November 2021) Wired, online:* **https://www.wired.com/story/mcdonalds-ice-cream-machine-hacking-kytch-taylor-internal-emails/** *accessed 10 July 2025.*

35 *Linda Xu & Ian Drew, "The great McDonald's ice cream machine meltdown: copyright, control, and the fight for repair rights" (28 February 2025) Davis Collision Cave, online:* **https://dcc.com/news-and-insights/the-great-mcdonalds-ice-cream-machine-meltdown-copyright-control-and-the-fight-for-repair-rights/** *accessed 8 July 2025.*

36 *For example, since the 1990s, virtually all cars produced globally have standardised on-board diagnostic ports ("OBD-II") that allow reading basic diagnostic trouble codes with generic scanners.*

37 *For example, Volkswagen's "ODIS" (Offboard Diagnostic Information System) is the official, dealer-level diagnostic software used by the Volkswagen Group to diagnose, repair, and program all its vehicle brands including VW, Audi, Skoda, and SEAT. This system connects directly to the manufacturer's German servers to provide technician with up-to-date fault codes, technical service bulletins, wiring diagrams, and other information. See, Technical Topics, 'ODIS VW Group Diagnostic Tool' (Technical Topics)* **https://techtopics.co.uk/odis-vw-group-diagnostic-tool/** *accessed 13 September 2025.*

38 *Maria Merano, "Tesla diagnostic software now available for purchase in the US" (26 August 2021) Teslarati, online:* **https://www.teslarati.com/tesla-diagnostic-software-right-to-repair-service/#:~:text=,greentheonly%29%20August%2026%2C%202021** *accessed 10 September 2025.*

39 *Jason Koebler, 'This Is Apple's Mysterious "iPhone Calibration Machine"' (VICE, 14 March 2017)* **https://www.vice.com/en/article/this-is-apples-mysterious-iphone-calibration-machine/** *accessed 13 September 2025.*

40 *Kevin Purdy, 'Here Are the Secret Repair Tools Apple Won't Let You Have' (iFixit, 28 October 2019)* **https://www.ifixit.com/News/33593/heres-the-secret-repair-tool-apple-wont-let-you-have** *accessed 13 September 2025.*

41 *Apple Support, 'Use Repair Assistant to finish an iPhone or iPad repair' (2 April 2025)* **https://support.apple.com/en-us/120579** *accessed 13 September 2025*

42 *One example of a lesser-known software tool of this sort is Samsung's "Must" application that is required for calibration and diagnostics on the manufacturer's Galaxy line of phones. For more on this, see Pr0Ankit, 'How to calibrate Force Touch on Samsung Galaxy S8' (XDA Developers Forum, 18 January 2018)* **https://xdaforums.com/t/how-to-calibrate-force-touch-on-samsung-galaxy-s8.3736990/** *accessed 13 September 2025.*

43 *SmartHQ Pro, 'Appliance Diagnostic Platform | SmartHQ™ Service' (SmartHQ Pro)* **https://www.smarthqpro.com/service** *accessed 13 September 2025.*

44 *SmartHQ Pro, 'Quick Start Guide: SmartHQ™ Service Setup' (SmartHQ Pro)* **https://www.smarthqpro.com/service/quick-start-guide** *accessed 13 September 2025.*

45 *'Refrigerator Diagnostics using the Updated SmartHQ Service Platform' (YouTube)* **https://www.youtube.com/watch?v=TjCLA0ydmoQ** *accessed 13 September 2025.*

46 *Elizabeth Chamberlain, 'Repairing a Fridge Costs More Than a Fridge' (iFixit, 23 November 2022)* **https://www.ifixit.com/News/69391/repairing-a-fridge-costs-more-than-a-fridge** *accessed 13 September 2025.*

47 *Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, art 26* **https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF** *accessed 14 September 2025.*

48 *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC [2024] OJ L, 28.6.2024, ELI:* **http://data.europa.eu/eli/reg/2024/1781/oj** **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1781** *accessed 10 September 2025.*

49 *Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products [2009] OJ L 285/10* **https://eur-lex.europa.eu/eli/dir/2009/125/oj/eng** *accessed 10 September 2025.*

50 *European Commission, 'Annexes 1–8 to the Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC' COM(2022) 142 final, 30 March 2022* **https://eur-lex.europa.eu/resource.html?uri=cellar:bb8539b7-b1b5-11ec-9d96-01aa75ed71a1.0001.02/DOC_2&format=PDF** *accessed 10 September 2025.*

51 *More specifically, Annex II includes household washing machines, dryers, refrigerators, electronic displays, welding equipment, vacuum cleaners, servers and data storage products, mobile phones and tablets, and 'goods containing light means of transport batteries'.*

52 *Importantly, these obligations under article 5 of the R2R Directive are limited to a relatively narrow group of products listed in Annex II. Those include household washing machines, dishwashers, refrigerators, electronic displays, welding equipment, vacuum cleaners, severs and data storage equipment, mobile phones and tables, electric bikes and scooters.*

53 *Commission Regulation (EU) 2023/1670 of 16 June 2023 laying down ecodesign requirements for smartphones, mobile phones other than smartphones, cordless phones and slate tablets pursuant to Directive 2009/125/EC and amending Commission Regulation (EU) 2023/826 [2023] OJ L 214/47* **https://eur-lex.europa.eu/eli/reg/2023/1670/oj/eng** *accessed 10 September 2025.*

54 *US Congress, 'Fair Repair Act' H.R. 4006, 117th Congress (2021–2022) (introduced 17 June 2021)* **https://www.congress.gov/bill/117th-congress/house-bill/4006** *accessed 10 September 2025.*

55 *For example, in 2021 the Federal Trade Commission (FTC) issued a policy statement committing to enforce against illegal repair restrictions, following a report that found many manufacturer-imposed repair barriers (like software locks) to be anti-competitive. Furthermore, President Biden's Executive Order 14036 (2021) also encouraged the FTC to address undue repair restrictions.*

56 *U.S. PIRG, 'RELEASE: All 50 states now have filed Right to Repair legislation over last 8 years' (PIRG Media Center, 24 February 2025)* **https://pirg.org/media-center/release-all-50-states-now-have-filed-right-to-repair-legislation-over-last-8-years/** *accessed 10 September 2025.*

57 *New York State Senate Bill S1320, 2023–2024 Regular Session, 'Relates to the sale of digital electronic equipment ...'* **https://www.nysenate.gov/legislation/bills/2023/S1320** *accessed 10 September 2025.*

58 *Minnesota Statutes § 325E.72 (2024) ('Digital Fair Repair Act')* **https://www.revisor.mn.gov/statutes/cite/325E.72** *accessed 10 September 2025.*

59 *Ibid, subd 6 (Exclusions).*

60 *Nathan Proctor, "Minnesota passes broadest Right to Repair measure to date" (24 May 2023) PIRG,* **https://pirg.org/articles/minnesota-passes-broadest-right-to-repair-measure-to-date**, *accessed 10 September 2025.*

61 *Colorado House Bill HB22-1031, 2022 Regular Session, 'Consumer Right To Repair Powered Wheelchairs'* **https://leg.colorado.gov/sites/default/files/2022a_1031_signed.pdf** *accessed 10 September 2025.*

62 *Colorado House Bill HB23-1011, 2023 Regular Session, 'Consumer Right To Repair Agricultural Equipment'* **https://leg.colorado.gov/sites/default/files/2023a_1011_signed.pdf** *accessed 10 September 2025.*

63 *Massachusetts, Acts 2013, ch 165, An Act relative to automotive repair* **https://malegislature.gov/Laws/SessionLaws/Acts/2013/Chapter165** *accessed 10 September 2025; Massachusetts, Acts 2020, ch 386, An Act to enhance, update and protect the 2013 motor vehicle right to repair law* **https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter386** *accessed 10 September 2025. .*

64 *California, Senate Bill 244 (2023–2024 Reg Sess), 'Right to Repair Act', ch 704, Statutes of 2023* **https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB244** *accessed 10 September 2025.*

65 *Daniel Rangel and Katie Hettinga, 'How Federal Trade Deals Threaten States' Crackdowns on Big Tech' (Governing, 17 September 2024)* **https://www.governing.com/policy/how-federal-trade-deals-threaten-states-crackdowns-on-big-tech** *accessed 20 July 2025.*

66 *Magdalena Słok-Wodkowska & Joanna Mazur, "Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code" (2022) 25 Journal of International Economic Law 91 at 96–98.*

67 *"Source Code Definition", Linux Information Project (14 February 2006), online: <***https://www.linfo.org/source_code.html#:~:text=Source%20code%20(also%20referred%20to,human%20readable%20alphanumeric%20characters**>

68 *Daniel Lin, Matthew Sag & Ronald S. Laurie, "Source Code versus Object Code: Patent Implications for the Open Source Community" (2002) 18:2 Santa Clara Computer & High Tech LJ 235–258 at 238.*

69 *Agreement between the European Union and Japan for an Economic Partnership [2018] OJ L 330/3, art 8.73* **https://eur-lex.europa.eu/eli/agree_internation/2018/1907/oj/eng** *accessed 8 September 2025.*

70 *Agreement on Digital Trade between the European Union and the Republic of Singapore (signed 7 May 2025) art 11* **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0022** *accessed 8 September 2025.*

71 *Ibid article 11(2)(c).*

72 *For example, a similar source code provision is found in the EU-UK Trade and Cooperation Agreement (2020). See, Trade and Cooperation Agreement between the United Kingdom of Great Britain and Northern Ireland and the European Union (signed 30 December 2020) art 207* **https://assets.publishing.service.gov.uk/media/608ae0c0d3bf7f0136332887/TS_8.2021_UK_EU_EAEC_Trade_and_Cooperation_Agreement.pdf** *accessed 8 September 2025.*

73 *World Trade Organization, "Joint Statement on E-Commerce", <***https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm***> accessed 8 September 2025.*

74 *David Lawder, "US drops digital trade demands at WTO to allow room for stronger tech regulation" (25 October 2023) Reuters, online:* **https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/** *accessed 8 September 2025.*

75 *For example, in presentations immediately following the U.S. reversal, Ambassador Tai commented that the USTR's concerns were influenced heavily by market competition, firm size, and other anti-trust considerations, indicating a novel confluence of policy considerations in the context of international trade. For a deeper analysis of these dynamics, see Alex Mastorides, "One Step Forward, Two Steps Back: The United States' New Direction on Digital Trade" (2025) 26:1 Minnesota Journal of Law, Science and Technology 116-203, 170-171.*

76 *Elizabeth Warren, Jan Schakowsky et al., 'Letter to President Biden in Support of USTR Digital Trade Work' (6 November 2023)* **https://www.warren.senate.gov/imo/media/doc/FINAL%20Letter%20to%20Biden%20in%20Support%20of%20USTR%20Digital%20Trade%20Work.pdf** *accessed 8 September 2025.*

77 *Kenneth Propp, "Transatlantic Digital Trade Protections: From TTIP to 'Policy Suicide'?" (16 February 2024) LawFare, online:* **https://www.lawfaremedia.org/article/transatlantic-digital-trade-protections-from-ttip-to-policy-suicide**, *accessed 8 September 2025.*

78 *European Commission, 'Digital trade'* **https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en** *accessed 8 September 2025.*

79 *Henry Gao, 'The Joint Statement on E-commerce: Is This Glass Half Empty or Half Full?' (Centre for International Governance Innovation, 30 September 2024)* **https://www.cigionline.org/articles/the-joint-statement-on-e-commerce-is-this-glass-half-empty-or-half-full/** *accessed 8 September 2025.*

80 *World Trade Organization, 'Joint Statement Initiative on Electronic Commerce: Communication from the Co-Convenors (Australia, Japan and Singapore)' INF/ECOM/87 (26 July 2024)* **https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True** *accessed 8 September 2025.*

81 *Samuel Stolton, "How trade commitments narrowed EU rules to access AI's source codes," Euractiv (17 January 2024)* **https://www.euractiv.com/news/how-trade-commitments-narrowed-eu-rules-to-access-ais-source-codes/** *accessed 7 October 2025.*

82 *For example, the EU-New Zealand agreement serves as an example of an increasingly permissive and public-interest facing approach to digital trade and 'source code' provisions negotiated recently by the EU.*

```
const artifactMesh = await initialize.
context.createBuffer({
    id: “genesis_0x7f4b”,
      type: “VERTEX”,
    size: 2048,
     format: ‘vec3<f32>’,
     attributes: [
       { name: ‘a_position’, offset: 0,
stride: 12 },
       { name: ‘a_normal’, offset: 12,
stride: 12 }
     ]
});



const { hyper_core, delta_stream } =
process.env;

frameTick) {
    if (metadata.status === ‘READY’) {
       const hash = ((frameTick &
```