Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

May 31, 2019

Via Electronic Submission

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Federal Trade Commission's "Nixing the Fix" Workshop

Microsoft Corporation ("Microsoft") appreciates the opportunity to provide information for the Federal Trade Commission ("FTC") to consider as it plans its "Nixing the Fix" Workshop. Founded in 1975, Microsoft develops and supports software, services, devices, and solutions that help people and businesses realize their full potential. Our products include: cloud services, operating systems, cross-device productivity applications, server and business solution applications, desktop and server management tools, software development tools, and video games. We also design, manufacture, and sell devices, including personal computers, laptop computers, tablets, gaming and entertainment consoles, other intelligent devices, and related accessories.

Microsoft designs our products to delight our customers, which means anticipating and addressing their needs and preferences. Our design decisions do not occur in a vacuum. We are required to consider and balance many competing factors that consumers value, including device functionality, product safety, security, interoperability, and quality. Microsoft also considers and promotes repairability and sustainability when designing its devices when such goals do not undermine or conflict with other important factors.

We encourage the FTC, when designing the workshop, to consider the complexity of product design decisions and to assess the trade-offs associated with "repair restrictions," as described in the notice. A wide variety of design choices that are made to meet consumer demands and market requirements may incidentally affect device repairability, but such design features serve other important purposes and should not be evaluated solely as "repair restrictions" in isolation from other design-related demands.

Microsoft product design characteristics—including aesthetic design choices—are primarily driven by consumer demand and preferences around device or platform functionality. As the FTC prepares for the workshop, we urge the FTC

to take a holistic approach to assessing product design choices adopted for reasons that benefit consumers, are based on consumer demand, or protect consumers' interests in a highly competitive market.

The electronic device market is highly competitive, and consumers have the freedom to choose devices that meet their needs and preferences. If repairability is an important factor, there are devices in the market that are readily repairable, and consumers can use their purchasing power to select such devices. Microsoft encourages the FTC to balance the consideration of these significant consumer benefits against any incidental impacts on the ability to repair such devices and to recognize that industry is already balancing these kinds of considerations when making product design decisions.

I.   Background on Microsoft and Its Products.

Microsoft devices include the Surface line of computers and other intelligent devices; Xbox gaming/entertainment consoles and accessories; HoloLens, a self-contained holographic computer; and personal computing accessories (mice, headsets, and keyboards).

Microsoft operates in a highly competitive and informed device market,[1] and it succeeds by designing and selling premium, high-quality, durable, and long-lived devices. Microsoft's market leadership is built on a strong relationship with its customers, who are free to choose from devices and software services from numerous competitors, and on delivering specific features and services desired by our customers. To support the goals of ensuring strong consumer relationships and delivering long-lived devices, Microsoft considers repairability and sustainability when designing devices, and the company offers to repair such devices, when necessary, at a reasonable cost. Microsoft also helps consumers extend the lifecycle of their devices through the use of firmware updates, including Windows Update, that enhance customer satisfaction and protection. Microsoft's Windows 10 operating system is licensed on a subscription basis, which means computer owners can keep the same hardware for years and receive regular Windows 10 updates to extend the life of the underlying device, while enhancing device security and delivering new and updated features.

II.   Scope of the FTC Workshop.

The FTC's request for comments on "repair restrictions" can be read as encompassing a broad and diverse set of business practices. In fact, many of the practices are design decisions aimed at improving the consumer experience. For example, the request for empirical research and data notes the use of "adhesives

---

[1] For example, third-party resources, including Consumer Reports or CNET, provide extensive information about consumer products, including quality, reliability, functionality and other performance ratings.

instead of machine screws when securing a part such as a battery."[2] As discussed in detail below, there are many pro-consumer design reasons for using an adhesive to affix a battery to a device enclosure, including product safety, product durability, battery protection, and extended battery life.

Designs or policies that may appear to limit self-repair or repair by an unauthorized agent should not be assumed to be harmful to consumers. Many design features sought by consumers, including for aesthetic, safety, security, or operability reasons, may have the secondary effect of making repairs more complex or challenging. However, design choices that incidentally impact repairability can also be innovative responses to consumer preferences and may form the basis on which companies compete. Today's highly complex, Internet-connected devices require design choices that deliver pro-consumer objectives, including safety, security, operability, and convenience. The fact that such designs may affect or limit repairs should not be considered anti-consumer and instead should be viewed holistically in terms of the benefits and choices provided to consumers.

For example, one company may choose to affix a battery in a certain way in order to maximize its size and power, enabling longer device run time; while another company may make batteries easier to replace, which might require a smaller battery, resulting in shorter run time. Computers and laptops are sold in a competitive marketplace, and consumers use their purchasing power to choose between competing designs based on the device performance factors that are most valuable to them. Manufacturers may elect to produce products that appeal to consumers who prefer product designs that offer easier repairability over other features. Voluntary ecolabel programs, such as participation in the EPEAT Registry, also provide a market-based incentive for manufacturers that provide such designs. Any regulatory action to restrict or direct design choices would reduce consumer choice and, therefore, competition in the marketplace.

These kinds of design decisions are far afield of the circumstances covered by the Magnuson-Moss Warranty Act,[3] which restricts the specific practice of conditioning warranties on requirements to use a certain branded product or service.[4] Indeed, that Act was passed because Congress was concerned that "the consumer has available to him little or no information about the product reliability

---

[2] *Call for Empirical Research: Nixing the Fix: A workshop on repair restrictions*, FTC, https://www.ftc.gov/nixing-the-fix-call-for-research.

[3] The legislation was spurred by a 1965 FTC investigation into whether "there was a significant failure of performance on the part of automobile manufacturers to live up to their warranty promises," S. Rep. No. 93-151, at 4 (1973). While it more broadly covers consumer products, what is considered the first commercially successful portable personal computer, the Osborne 1 (a computer the size of a suitcase; weighing more than 23lbs) was not released until six years after the Act was passed. Lincoln Spector, *A History of Portable Computing*, PC WORLD (May 31, 2010) https://www.pcworld.com/article/197457/History_of_Portable_Computing.html#slide2. Microsoft's first version of Windows was not released until four years after that, in 1985.

[4] 15 U.S.C. § 2302(c).

potential of any consumer product," including warranty conditions,[5] but consumers can now access the Internet to readily compare warranties, repair options, and product reliability when they are researching a device for purchase.

Any action by the FTC to regulate, authorize, or guide specific design elements will limit competition and stifle innovation among product manufacturers. Not only will such action discourage product manufacturers from competing based on certain product features and design elements, it will also limit product developers' ability to respond to future consumer demand. Recent history has demonstrated that it is difficult to predict today which design elements will be the most important for consumers tomorrow. Stifling the ability of the device industry to innovate and produce new designs and construction techniques will negatively impact industry, consumers, and the market. We urge the FTC to carefully weigh the costs and benefits of any potential regulatory action or agency recommendation and evaluate whether consumers have suffered a cognizable harm from any act or practice.[6]

Finally, we note that the FTC's workshop potentially encompasses the bases for not only current design decisions, but also those underlying the safety, security, and operability of billions of devices, which have yet to be designed and manufactured. Today the burgeoning Internet of Things ("IoT") market has made connectivity the norm, as analysts predict that there will be more than 64 *billion* IoT devices globally by 2025.[7] The majority of these IoT devices will have consumer applications.[8] Each of these devices may include designs that have the effect of limiting consumer repair for safety, security, or operability reasons. The FTC should be cautious about taking any action that could stifle innovation or competition or limit design choice in this emerging IoT market.

---

[5] S. Rep. No. 93-151, at 8 (1973).

[6] "The FTC has long used its broad authority under Section 5 of the FTC Act to address *consumer harms* arising from new technologies and business practices . . ."*Prepared Statement of the Federal Trade Commission: "Oversight of the Federal Trade Commission" Before the Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection*, at 4 (July 18, 2018) (emphasis added), *available at* https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf; *see also "Our American Privacy": Remarks of Commissioner Noah Joshua Philips, U.S. Chamber of Commerce and the American Chamber of Commerce to the European Union*, at 5 (Oct. 23, 2018), *available at* https://www.ftc.gov/system/files/documents/public_statements/1421513/phillips_-_our_american_privacy_10-23-18_0.pdf (in the context of privacy enforcement: "Ours is standards-based, outcome-oriented, flexible approach, focused on consumer harm and capable of protecting consumers from harmful practices even as technologies develop and evolve in unanticipated ways.").

[7] Peter Newman, *IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers*, BUSINESS INSIDER (Jan. 28, 2019), https://www.businessinsider.com/internet-of-things-report.

[8] *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, GARTNER (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

III.   Additional Information Relevant to the Workshop.

The FTC has sought information on justifications for "repair restrictions." Below, we discuss the pro-consumer reasons why Microsoft makes certain design choices that may have collateral effects on device repairability. These include enhancement of functionality, quality, durability, and sustainability; protecting user safety; protecting device and network security; combatting unlawful piracy of intellectual property; and promoting fairness on gaming platforms. It is important to note that Microsoft does consider repairability as a design factor but only in conjunction with these other factors.

A.   <u>Design Choices Are Driven by Consumer Demand for Superior Functionality, Quality, Durability, and Sustainability</u>.

Microsoft designs its products—including its Surface family of products—based on customer demand for high quality products. Our customers demand mobile products that are thin and light, durable and long-lasting, and have maximum possible usage times (i.e., hours of use before recharging the battery). Indeed, our customer surveys show that customers highly value the portability, lightness, and functionality of the Surface line of devices in making their purchasing decisions. To remain competitive, Microsoft's product designers continuously develop novel solutions to the engineering challenges presented by these customer expectations.

For example, Microsoft makes numerous design decisions about the size and installation of its batteries, including the use of adhesives. The top consumer demand that influences battery design choices is long run time. Maximizing the consumer's usage time without recharging the battery requires a device to contain the largest battery capacity possible, which requires the battery's physical dimensions (e.g., size and thickness) to be maximized within the constraints of the interior casing. Microsoft and many other device manufacturers utilize "pouch" lithium ion cells, which eliminate unnecessary bulk, and are designed to achieve exact tolerances between the product casing and the battery. Pouch cells also require the use of adhesives because the pouch does not contain rigid material that could be used to screw the battery in place. Moving to a rigid battery design that could be secured using screws, instead of adhesive, would require a reduction in the power-providing portion of the battery, reducing the energy capacity of the battery and device run time. We estimate that use of a rigid battery design would result in a reduction of battery life of up to 1.4 hours for the average user – a reduction that would be unacceptable to most Microsoft customers who highly value long run time.

A decision to use adhesives is also driven by product reliability and durability demands. The use of adhesives to affix batteries or display panels increases the structural integrity of devices, improving damage resistance and enhancing product durability. Compared to screw-down solutions that offer only a

few points of contact to secure components to the casing, adhering components significantly improves overall product durability during everyday use, including inadvertent drops or mishandling. Adhesives also meet consumer demand for a high-quality, tactile, and "solid" product feel by preventing internal components from rattling within the casing.

        B.   <u>Many Design Decisions are Made to Protect Consumer Safety</u>.

Microsoft designs its products with consumer safety as a priority. Microsoft devices, like other consumer products, are highly complex and integrated, containing multiple components that, if taken apart and handled improperly, could lead to serious injuries, including severe burns. The lithium ion batteries in Surface products and some accessories, if handled improperly or damaged during a repair, could create fire hazards.[9]

As the Consumer Product Safety Commission ("CPSC") has noted, "[h]igh-energy density batteries need enhanced safety systems and additional care when using and handling, both in or when removed from the product; and batteries must be properly tested with the product, in its intended use and with the charger as a system."[10] Thus, maintaining the physical protection of a lithium ion battery is a critical design and safety consideration for any modern mobile device.

The use of exact spatial tolerances between the battery and the casing and the use of adhesives to secure the battery both promote battery safety. Adhesives not only make the product more durable, as noted above, but also provide additional safety protections by preventing the battery from moving during normal use, including situations where the device is dropped or otherwise damaged. This helps to limit the potential for damage to the battery, which could create a safety hazard. As a result, spatial tolerances are inspected using precise optical technology at assembly factories, and devices which fail to meet those tolerances are rejected for safety reasons.

When Microsoft or its authorized repair providers repair devices, they use replacement batteries that meet Microsoft specifications to avoid problems caused by subpar or counterfeit replacement batteries,[11] they meet strict quality and safety

---

[9] *See e.g.,* Richard Chirgwin, *Loose screw caused airplane iPhone 'fire'*, THE REGISTER (May 6, 2012, 11:15 P.M.), https://www.theregister.co.uk/2012/05/06/screw_caused_iphone_fire/.

[10] *Batteries*, U.S. CONSUMER PRODUCT SAFETY COMMISSION (2018), https://cpsc.gov/Regulations-Laws--Standards/Voluntary-Standards/Topics/Batteries/; *see also* Douglas Lee, Status Report on High Energy Density Batteries Project (Feb. 12, 2018), https://www.cpsc.gov/s3fs-public/High_Energy_Density_Batteries_Status_Report_2_12_18.pdf.

[11] Additionally, installation of counterfeit batteries can create significant safety risks. *See, e.g., Electrical Fire Recall*, U.S. CONSUMER PRODUCT SAFETY COMMISSION (Aug. 16, 2017), https://www.cpsc.gov/recall-hazards/electrical-fire (recalling refurbished cell phone batteries because "some of the recalled batteries are counterfeit and show anomalies that can lead to overheat"); Dave Etchells, *Counterfeit batteries: Clever fakes, uncertain risks*, IMAGING RESOURCE (Oct. 28, 2015, 6:51 P.M.), https://www.imaging-resource.com/news/2015/10/28/counterfeit-battery-

standards to ensure proper repair, and they follow specific repair procedures to avoid creating potential safety risks caused by damaged batteries or improperly installed batteries.

Microsoft frequently receives devices returned by consumers for failures caused by third-party repairs. The use of off-specification batteries and power supply units, which do not meet Microsoft's quality standards, are regularly identified as the cause of device overheating or other potential safety hazards in returned devices. For example, over the past 3 years, Microsoft has received at least 12 reports of serious overheating incidents and device damage caused by off-specification or counterfeit power supply units (i.e., the power cord and "brick" that plugs into the device) for its Surface products. Over the same period, Microsoft has not identified any similar incident reports for the certified power supply units manufactured by Microsoft.

The concerns associated with power supply safety recently prompted the CPSC, Health Canada, and PROFECO (Mexico) to evaluate the safety of aftermarket AC and USB power supply units. Their work noted the frequent inability of power supply units to meet industry standards, particularly among chargers which had not been evaluated and certified by a third-party testing facility.[12]

All Microsoft original and replacement power supplies are certified, UL listed, and designed to meet industry standards for safety, reliability, and performance. This is a critical factor for Microsoft. There is simply no way to ensure that independent or unauthorized providers will provide certified, UL listed, and industry standard replacement parts when conducting repairs, raising safety risks to consumers.

C.   Microsoft Design Decisions Enhance Device and Platform Security and Protection of User Data.

Microsoft is highly focused on the security of its devices and platforms and devotes enormous resources to protecting devices from cybersecurity threats and malicious hacks. These sorts of threats can directly compromise the privacy of consumers, including exposing personal information and data to unauthorized persons. Many electronic devices are designed to operate as an integrated system.

---

fakes-with-risks; *Counterfeit Product Alert, Lithium Ion: 18650 Batteries* (Apr. 4, 2019), https://thecounterfeitreport.com/product/642/Lithium-Ion-18650-Batteries.html; *Woman Sentenced For Selling Counterfeit Samsung Batteries*, U.S. DEPARTMENT OF JUSTICE, U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF TEXAS (Apr. 17, 2015), https://www.justice.gov/usao-sdtx/pr/woman-sentenced-selling-counterfeit-samsung-batteries.

[12] *CPSC, Canadian, Mexican Consumer Safety Counterparts Create Consensus Recommendations on Product Testing*, U.S. CONSUMER PRODUCT SAFETY COMMISSION (Apr. 3, 2019), https://www.cpsc.gov/Newsroom/News-Releases/2019/CPSC-Canadian-Mexican-Consumer-Safety-Counterparts-Create-Consensus-Recommendations-on-Product-Testing.

The unauthorized repair and replacement of device components can result in the disabling of key hardware security features or can impede the update of firmware that is important to device security or system integrity. Moreover, a security breach of one device can potentially compromise the security of a platform or other devices connected to the network.[13]

The Commission has long been at the forefront of encouraging companies to incorporate appropriate cybersecurity protections. It has also recognized the importance of maintaining security throughout the lifecycle of a device and encouraged manufacturers to exercise diligence over service providers whose activities could affect device security. Staff has noted, for example, that "[c]ompanies should provide oversight by exercising due diligence in their selection of service providers, incorporating security standards into their contracts, and taking reasonable steps to verify compliance with those security standards on an ongoing basis."[14] The agency has also counseled that "companies should take reasonable steps to address threats to privacy, security and safety after launching products, including by issuing updates and patches."[15]

Installation of counterfeit or defective replacement parts can hinder device operations and compromise device security. Microsoft carefully tracks the chain of custody of all components in our device supply chains for security purposes. Additionally, Microsoft provides our trusted original and replacement hardware manufacturers access to proprietary integrated security measures intended to ensure that replacement parts are fully compatible with our devices.

Microsoft computing hardware products utilize a Trusted Platform Module ("TPM"), which is an embedded hardware security technology that provides high-grade cryptographic protections for user data and checks that device integrity is maintained during boot up and that no unexpected changes to hardware are detected.[16] The TPM works in conjunction with the integrated security measures to provide a mechanism to stop malicious hardware components from being installed in our devices. Microsoft technologies, like Windows Defender, rely on trusted hardware components, like the TPM, to protect consumers from malicious threats. If the TPM or other similar hardware and software protections were compromised

---

[13] *See* Crowdstrike Cyber Intrusion Services: Casebook 2018, at 11, *available at* https://crowdstrike.lookbookhq.com/casebook-web-download/cs-services-casebook-2018 (describing case study in which one "infected laptop served as the entry point for the adversary to compromise . . . [a] corporate network").

[14] Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection FTC, Docket No. CPSC-2018-007, at 7 (Jun. 15, 2018).

[15] *Id.* at 8.

[16] Andrea Bichsel, et al., *Trusted Platform Module Technology Overview*, MICROSOFT (Nov. 28, 2018), https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

by a malicious or unqualified repair vendor, those security protections would be rendered ineffective and consumers' data and control of the device would be at risk.

It is therefore critical for electronic devices to be serviced by knowledgeable, trained professionals who understand how to repair products without disabling the hardware and software features that protect the device from external security threats. This requires training and use of authorized parts and approved procedures.[17]

In addition to the risk of a security compromise, consumers face significant risks when they provide a device containing sensitive personal information to an independent or unauthorized repair provider. A personal computing device, such as a Surface, may contain a user's pictures, sensitive documents, financial records, emails, passwords, and personal contacts. An independent repair facility that has access to the device's hardware may be able to recover and misuse this personal data. Users have little visibility into or control over what independent or unauthorized third repair providers might do with their devices. There are no standards for independent repair that would provide consumers with protection, assurances, or possible opportunities for redress should their personal data be misappropriated.

D.   Design Decisions Are Made to Protect Intellectual Property and Combat Illegal Software Piracy.

Microsoft also designs its devices to safeguard the software from piracy. Microsoft device protections help Microsoft protect copyrights to some of the world's most successful (and unfortunately, most pirated) software products in history, including Windows and Microsoft Office. These protections also play a key role for the tens of thousands of (i) software developers and publishers, which distribute their apps and games via Microsoft's online Windows Store for use on hundreds of millions of PCs, tablets and mobile devices; and (ii) motion picture, music, and video game copyright owners whose works are used on Xbox video game consoles and distributed via Xbox Live online platforms.

Unscrupulous third parties have been known to seek ways to modify Xbox devices to permit a user to play a pirated game or engage in unauthorized copying of movies or games, and Microsoft's Office products have been the subject of piracy efforts for decades. This kind of activity is not only unlawful,[18] but software piracy imposes enormous costs on publishers and ultimately consumers. In fact, protecting software from piracy benefits consumers by encouraging innovation and

---

[17] Moreover, as noted above, even outside of Microsoft devices, the popularity and use of other IoT devices are expected to increase exponentially. IoT devices will be widely used for varied purposes such as tracking health, ordering groceries, monitoring infants, and maintaining home security – among many other purposes where important consumer data is gathered and could be vulnerable if device or platform security is circumvented.

[18] 17 U.S.C. § 501 ("Infringement of copyright").

software development – for example, by encouraging game developers to produce games for Microsoft's Xbox platform.

Piracy concerns are hardly unfounded. For example, malicious actors identified methods to use alternative hardware firmware to circumvent the antipiracy measures Microsoft used on its Xbox 360 gaming console. In that device, Microsoft worked to prevent piracy by using customized DVD drive firmware, which used a proprietary method of determining whether an inserted game disc was a validly purchased version or an illegal copy. Malicious actors identified and widely disseminated a method of disabling that protection to allow the use of illegally copied game discs. See, for example:

- https://www.se7ensins.com/forums/threads/flashing-your-xbox-360-beginner-faq-please-read-first.41684/
- https://www.se7ensins.com/forums/threads/how-to-replace-spoof-a-xbox-360-dvd-drive.32679/
- https://www.se7ensins.com/forums/forums/xbox-360-firmware-modding-tutorials.90/

Microsoft learned from these malicious acts and developed more robust piracy protections in the current generation of Xbox One devices. Microsoft allows only specific trusted hardware vendors to have access to the technical details which provide these protections. While Microsoft does not know how malicious actors first discovered the techniques used in the past to enable illegally copied game discs, experience has proven that unfettered access to diagnostic and proprietary hardware tools increases the potential for malicious actors to circumvent anti-piracy controls.

E.   Device Designs Promote Fairness in Gaming.

Device measures can also safeguard device software from being modified to allow users to "cheat" at online games. While the vast majority of Xbox users do not attempt to cheat, a certain subset of individuals involved in online gaming seek an improper advantage over other players. As the operator of the Xbox Live online gaming platform and the developer and publisher of popular competitive games, Microsoft has found that some unprincipled game players—representing a small subset of users—seek unfair advantages through "cheats" such as the modification of game code or game consoles. This activity is unlawful[19] and it degrades the user experience by disadvantaging other players. Indeed, users who participate in Microsoft's Xbox Live online gaming platform have an expectation that the Xbox service will be provided in a fair manner.

To prevent the unauthorized modification of gameplay components, Microsoft has adopted heightened software authorization and security protocols for

---

[19] *See* 17 U.S.C. § 1201.

its Xbox One hardware compared to prior generations of devices. These kinds of protections again are often embedded in proprietary software and hardware. As noted above, in the past, Microsoft has seen unscrupulous third parties compromise device firmware or software restrictions on older devices to bypass security measures to cheat in gameplay. Tutorials on these exploits and hacks promote gameplay cheating as a primary goal. For example:

- https://www.se7ensins.com/forums/threads/how-to-hack-xbox-360-achievements-using-xbox-360-profile-editor-by-carson.82038/
- https://www.se7ensins.com/forums/threads/how-to-mod-achievements-on-xbox-360-new-and-updated.690919/
- https://www.se7ensins.com/forums/threads/jtag-rgh-r-jtag-xbox-360-ultimate-exploit-guide.804054/
- https://www.se7ensins.com/forums/threads/how-to-get-online-with-your-rgh-jtag-r-jtag-console.1522743/

Providing third parties unfettered access to diagnostic tools for devices would inevitably lead to bad actors gaining access to those tools for the purpose of game cheating, thereby degrading the gaming experience sought by the clear majority of Xbox users and potentially reducing consumer loyalty to the platform.

IV.   Conclusion

Microsoft considers many factors when designing its devices. Our device design choices are primarily based on consumer demand and preferences for numerous product features, many of which require balancing potentially conflicting design choices to meet those demands. Repairability is one of those competing features. Microsoft strives to design repairable and sustainable devices, but consumers also demand features that drive design choices which may have the effect of impacting or impeding repairability.

Microsoft has compelling economic incentives to make sure that its customers remain satisfied with the aesthetics, functionality, safety, and security of our devices and that any repairs are completed promptly, effectively, and safely. A competitive and innovative market in which device design choices are driven by consumer demand and preferences and market competition and innovation will provide consumers with the most choice and empower them to use their purchasing power to select the devices that possess the features that they value most highly.

Thank you for this opportunity to provide Microsoft's perspective on this issue. We look forward to the workshop.