



Best Practices to Combat Online Sale of Counterfeits in the EU and US

By Becca Trate and Daniel Castro | July 13, 2022

E-commerce has significantly improved the way consumers buy goods, allowing for more choice and convenience, but bad actors can exploit online marketplaces—e-commerce platforms that allow for third-party sellers—to introduce counterfeit goods that can threaten public health, safety, and national security, as well as cause economic harm to legitimate businesses and their workers. To address this problem, policymakers in both the United States and the European Union have worked with the private sector to identify best practices to combat the sale of counterfeit goods.

As policymakers worldwide explore new anti-counterfeiting measures in their regions, a consensus is emerging in the United States and the EU on best practices for e-commerce platforms to combat online sales of counterfeit goods. These include: establishing and enforcing policies to protect IP rights; creating notice and takedown procedures; assessing third-party sellers; addressing pervasive counterfeit products proactively; preventing repeat offenders; enabling consumer reporting of counterfeits; providing redress for consumers receiving counterfeits; improving data sharing; and assisting law enforcement.

INTRODUCTION

E-commerce has significantly improved the way consumers buy goods, allowing for more choice and convenience, but bad actors can exploit online marketplaces—e-commerce platforms that allow for third-party sellers—to introduce counterfeit goods that can threaten public health, safety, and national security. Counterfeit goods are imitations of real products, often of an inferior quality, that use another brand's name without permission. Criminals use these fake or unauthorized replicas to profit unfairly from a

legitimate business's trademark, hurting a company's reputation and value. In many cases, consumers may be unaware that they have purchased a counterfeit product. As of 2019, international trade in counterfeit goods amounted to nearly half a trillion dollars or 2.5 percent of global trade.¹ To protect both consumers and rights holders, policymakers in both the United States and the European Union (EU) have worked with the private sector to identify best practices to combat the sale of counterfeit goods.

In the EU, the European Commission facilitated stakeholder dialogues between intellectual property rights owners, online platforms, and trade associations with the goal of creating a voluntary agreement to combat counterfeiting that was “realistic, balanced, proportionate, and fair for all concerned.”² In response, the stakeholders created the 2011 Memorandum of Understanding (MoU) on the sale of counterfeit goods on the Internet. The MoU contains key commitments by both online platforms and rights holders to prevent the sale of counterfeit goods by relying on notice and takedown procedures, proactive preventative measures, and cooperation with law enforcement.³ The MoU also includes a moratorium on new litigation between platforms and rights holders to promote the good-faith fight against counterfeit goods—those who signed agreed to not launch new litigation against each other in relation to matters of counterfeit goods.⁴ Stakeholders revised the MoU in 2016 to add key performance indicators (KPIs) to assess implementation of its provisions.⁵ As of October 2021, 32 companies and trade associations have signed the updated MoU.⁶

In the United States, President Trump issued the “Memorandum on Combating Trafficking in Counterfeit and Pirated Goods” in 2019 as a call to action to fight against counterfeit goods in American e-commerce markets.⁷ The memorandum directed the Department of Homeland Security (DHS) to produce a report offering recommendations for the government and private sector to address the sale of counterfeit goods, which DHS did in January 2020.⁸ The report, developed after extensive consultation with the private sector, included ten best practices for e-commerce platforms and third-party marketplaces. U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and National Intellectual Property Rights Coordination Center (IPR Center) subsequently published a summary of various steps industry stakeholders have taken to implement these best practices.⁹

BEST PRACTICES

The following summarizes best practices found in both the EU's MoU and the U.S.'s DHS report. They include: establishing and enforcing policies to protect intellectual property (IP) rights; creating notice and takedown procedures; assessing third-party sellers; addressing pervasive counterfeit products proactively; preventing repeat offenders; enabling consumer reporting of counterfeits; providing redress for consumers receiving counterfeits; improving data sharing; and assisting law enforcement.

ESTABLISHING AND ENFORCING POLICIES TO PROTECT IP RIGHTS

Both the United States and the EU recommend that platforms establish detailed policies for their sellers to protect IP rights.

UNITED STATES

“It is critical that platforms require all third-party sellers to sign comprehensive and stringent terms-of-service agreements that maximize the authorities of the platforms to combat counterfeit trafficking.”¹⁰

“...terms of service should incorporate explicit prohibitions on selling counterfeit and pirated goods and list the potential repercussions sellers face for violations. Generally, these repercussions should allow platforms to impose sanctions such as suspension, termination, and debarment without waiting for a determination by a court for sellers who violate the terms of the agreement. The terms should include escalating capabilities to suspend, terminate, and debar counterfeit traffickers and their affiliates.”¹¹

EUROPEAN UNION

“Internet Platforms commit to adopt, publish and enforce IPR policies, which should be clearly communicated and indicated on their sites and reflected in the contracts which they conclude with their sellers.”¹²

The U.S. best practices states that platforms should require all third parties to sign on to a “comprehensive and stringent” terms-of-service agreement, while the EU’s MoU states that platforms should enforce IP rights in their contracts with their sellers. Both the U.S. and EU best practices also call for platforms to enforce their terms of service to prevent the sale of counterfeits, with the U.S. best practices explicitly stating that penalties for violations should escalate and including suspension and termination of seller accounts.

CREATING NOTICE AND TAKEDOWN PROCEDURES

Both the United States and the EU emphasize the importance of creating a notice and takedown process that allows rights holders to efficiently report counterfeit listings, receive prompt action, and learn of the response.

UNITED STATES	EUROPEAN UNION
<p>“...platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns of infringing seller profiles and product listings. An effective regime should include, at a minimum, the following:</p> <ol style="list-style-type: none">1. minimal registration requirements for an interested party to participate in the notice and takedown process;2. reasonable rules that treat profile owners offering large quantities of goods on consumer-to-consumer platforms as businesses; and3. transparency to the rights holders as to how complaints are resolved along with relevant information on other sales activity by the seller that has been implicated.”¹³	<p>“...Internet Platforms commit to offer efficient and effective NTD [notice and take-down procedures], which should be accessible through electronic means. They should be: accessible via the website of the Internet Platform, understandable, not excessively burdensome and simple to subscribe to, complete and process.”¹⁴</p> <p>“Internet Platforms and Rights Owners commit to provide each other with feedback on their notifications. Relevant sellers should also be informed where an Offer has been taken down, including the underlying reason, and should be provided with the means to respond including the notifying party’s contact details provided by Rights Owners to Internet Platforms for this purpose.”¹⁵</p> <p>“Internet Platforms commit to deal with notifications in an efficient and comprehensive manner, without undue delay and to ensure that valid notifications of Offers of Counterfeit Goods lead to a swift removal or disabling of the notified Offer (take-down) and to take deterrent measures in relation to such sellers...”¹⁶</p>

Rights holders play an important role in policing online marketplaces for counterfeits, and therefore it is essential that they can efficiently submit infringement notifications. The U.S. best practices direct platforms to create a notice and takedown system that allow rights holders to easily participate. Likewise, the EU’s MoU commits signatory platforms to create a notice and takedown process that is “understandable, not excessively burdensome, and simple.”¹⁷ The EU’s MoU also specifies that reporting process should be accessible online. The U.S. best practices call for “quick and efficient” takedowns, while the EU states that platforms should ensure that valid complaints “lead to a swift removal.”¹⁸ Finally, the United States directs platforms to provide transparency on how they resolve complaints. Similarly, the EU specifies that platforms need to explain how a notification has been resolved.¹⁹

Because the EU’s MoU is between rights holders and platforms, whereas the U.S. DHS report is only directed at platforms, it includes additional stipulations about the responsibilities of rights holders, such as the responsibility to notify in good faith and liability if rights holders abuse the notice system. The EU’s MoU also notes the need for the platform to communicate with sellers to explain the reason for listing removals and to provide sellers an opportunity to respond.²⁰

ASSESSING THIRD-PARTY SELLERS

Both the United States and the EU outline the need for platforms to pro-actively prevent the sale of counterfeits by screening third-party sellers who operate on the platform.

UNITED STATES

“Platforms should have a uniform and articulable vetting regime to determine if a seller will be allowed to list products for sale. To facilitate enhanced vetting, platforms should, at a minimum, require the following:

1. sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform;
2. certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit or pirated products online; and
3. acknowledgment, where applicable, that the seller is offering trademarked products for which the seller does not own the rights (either because they are a reseller or seller of used products).”²¹

“Information provided by potential sellers should also be vetted for accuracy, including through the following efforts:

1. use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and
2. establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics.”²²

EUROPEAN UNION

“...Internet Platforms commit to take commercially and technically reasonable steps to request seller contact information and to verify this information, provided by sellers, in specific circumstances that warrant such identification, in order to gain a reasonable assurance of a seller’s identity.”²³

The U.S. best practices calls for platforms to develop a clear “vetting regime” to determine if sellers should be allowed to list on their platforms. It instructs platforms to assess the accuracy of the data, including through the use of data analytics and risk-based audits. Similarly, the EU MoU states that platforms should take “commercially and technically reasonable steps” to request and verify seller contact information when warranted.

Unlike the EU MoU, the U.S. best practices outline specific information a platform should collect from third-party sellers before they can join a marketplace, including seller identification, additional accounts it operates, and the physical location of its business. In addition, platforms should also require sellers to self-certify where it has been banned for selling counterfeit products on other platforms and to acknowledge if it is selling trademarked products for which it does not own the trademark.

ADDRESSING PERVASIVE COUNTERFEITS PROACTIVELY

The United States and the EU both outline the need for platforms to take proactive measures to address pervasive counterfeit products.

UNITED STATES

“Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of being counterfeited or pirated and/or pose a higher risk to the public health and safety. Platforms should prominently publish a list of items that may not be sold on third-party marketplaces under any circumstances (prohibited), as well as a list of items that can only be sold when accompanied by independent third-party certification (restricted). In constructing these lists, platforms should consider, among other things, whether a counterfeit version of the underlying product presents increased risks to the health and safety of U.S. residents or the national security of the United States.”²⁴

EUROPEAN UNION

“Internet Platforms commit to take appropriate, commercially reasonable and technically feasible measures, taking into consideration their respective business models, to identify and/or prevent proactively the sale of Counterfeit Goods, especially obvious Counterfeit Goods, and to prevent such goods being offered or sold through their services. The measures taken by Internet Platforms shall be at their discretion.”²⁵

“Rights Owners commit to take commercially reasonable and available steps to provide and update general information to Internet Platforms giving priority to specific products that Rights Owners contend present a substantial and pervasive Counterfeit Goods problem on that Internet Platform, including those products which are particularly susceptible to constituting Counterfeit Goods (such as products or ranges/ measures of products that do not exist in a Rights Owners’ product line but have been specifically developed by counterfeiters to attract consumers).”²⁶

“Rights Owners commit to provide to Internet Platforms at their request a list of keywords commonly used by sellers for the purpose of offering for sale obvious Counterfeit Goods, to assist Internet Platforms, as appropriate, with their Proactive and Preventive Measures.”²⁷

The U.S. best practices direct platforms to create procedures to address high-risk items, i.e., products that are at high risk of being counterfeit or pose a high risk to health and safety of consumers. Similarly, the EU MoU directs platform to take “appropriate, commercially reasonable and technically feasible measures” to proactively identify counterfeit goods, especially “obviously” counterfeit goods.”²⁸ The EU MoU also instructs rights holders to give information to platforms about any “substantial and pervasive” counterfeit goods on a given platform or are “particularly susceptible” to counterfeiting.”²⁹

In contrast to the EU, the U.S. best practices instruct platforms to publish a list of prohibited and restricted items, considering whether counterfeit versions of these items present a risk to consumer health and safety or national security.

PREVENTING REPEAT OFFENDERS

Both the U.S. and EU best practices direct platforms to address sellers who repeatedly sell counterfeit products.

UNITED STATES

“Platforms should require sellers to provide the names of their underlying business or businesses (if applicable), as well as any other related seller profiles owned or controlled by that seller or that clear transactions through the same merchant account.”³⁰

“...allow for an escalating enforcement structure that results in (for major infractions and/or repeat minor infractions) permanent removal of the seller, and any known related seller profiles, from the marketplace feature of the platform and further results in forfeiture and destruction of all offending goods in warehouses or fulfillment centers operated by, or under the control of, the platform.”³¹

EUROPEAN UNION

“Internet Platforms commit to implement and enforce deterrent repeat infringer policies, according to their internal guidelines. These policies should be enforced objectively and include the suspension (temporary or permanent) or restriction of accounts or sellers. Internet Platforms commit to use their best efforts to prevent re-registration of permanently suspended sellers. These policies should take particular account of factors, such as the severity of a violation, the number of alleged infringements (not taking into account the Offers deleted upon unjustified notification), the apparent intent of the alleged infringer and the record of notices and feedback, received from Rights Owners.”³²

“Subject to applicable data protection laws, Rights Owners commit to provide information to Internet Platforms concerning those sellers they believe to be repeat infringers and commit to provide feedback to Internet Platforms on the effectiveness of Internet Platforms’ policies regarding repeat infringers.”³³

The U.S. best practices instruct platforms to track seller IDs and remove sellers who repeatedly violate its policies, including any other profiles owned or controlled by that seller. Tracking seller IDs allows platforms to swiftly remove all accounts associated with a violation and prevent offenders from jumping between several accounts. The EU MoU similarly commits platforms to identify and remove repeat infringers, as well as prevent known infringers from re-registering on their platforms.

Since the EU MoU is an agreement between both platforms and rights holders, it also specifies that rights holders are responsible for informing platforms of repeat offenders and providing feedback on the effectiveness of platform policies.³⁴

ENABLING CONSUMER REPORTING OF COUNTERFEITS

Both the U.S. and EU best practices direct platforms to allow consumers to report counterfeits.

UNITED STATES

“Platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns of [counterfeit] seller profiles and product listings. An effective regime should include, at a minimum, the following: (1) minimal registration requirements for an interested party to participate in the notice and takedown process...”³⁵

EUROPEAN UNION

“Internet Platforms and Rights Owners recognize that consumers can be active parties in the fight against counterfeiting. They jointly recognize that consumers need to be provided with appropriate tools to help them report Offer of Counterfeit Goods and rogue sellers.”³⁶

“Internet Platforms and Rights Owners commit to provide appropriate means to consumers to identify and report Offers of Counterfeit Goods, prior to, or after purchase, to Internet Platforms and to Rights Owners.”³⁷

The EU MoU clearly specifies that platforms should provide means for consumers to identify and report counterfeits, including before or after purchase. In contrast, the U.S. best practices state that any “interested party” should be able to participate in the platform’s notice and takedown process, which presumably includes consumers.

PROVIDING REDRESS TO CONSUMERS

Both the United States and the EU direct platforms to provide redress for consumers who have purchased counterfeit products.

UNITED STATES

“Upon discovery that counterfeit or pirated goods have been sold, platforms should conduct a series of ‘post-discovery’ actions to remediate the fraud. These should include...notification to any buyer(s) likely to have purchased the goods in question with the offer of a full refund...”³⁸

“...e-commerce platforms should require foreign sellers to provide some form of security in cases where a foreign product is sold to a U.S. consumer. Such form of security should be specifically designed to cover the potential types and scope of harm to consumers and rights holders from counterfeit or pirated products.”³⁹

EUROPEAN UNION

“Internet Platforms recognize the importance of consumer confidence and satisfaction. To this end, they commit to assist consumers who unintentionally purchase Counterfeit Goods on their website.”⁴⁰

The U.S. best practices call for platforms to notify consumers who have purchased counterfeit items and provide them a full refund. Similarly, the EU’s MoU states that platforms should “assist” consumers who unintentionally purchase counterfeit products on their websites. The MoU does not explicitly state that buyers should receive a refund, but many platforms do.⁴¹

Both policies support the same goals of involving consumers in identifying and reporting counterfeit goods. The U.S. best practices place greater emphasis on consumer transparency. For example, additional U.S. best practices direct platforms to require sellers to disclose the country of origin of the products they sell; allow consumers to inspect seller profiles owned by the same underlying business; and prominently disclose when third-party sellers fulfill an online purchase.

U.S. best practices also call for platforms to require foreign sellers to provide some kind of indemnification for consumers, such as insurance covering harm to consumers and rights holders from counterfeit products, since domestic consumers and rights holders may not be able to seek redress effectively from overseas sellers.

IMPROVING DATA SHARING

The U.S. and EU best practices both call for better data sharing between stakeholders to combat counterfeits.

UNITED STATES

“... the IPR Center established the E-Commerce Working Group (ECWG) to foster and encourage the flow of actionable data and information between platforms and relevant third-party intermediaries as well as affected carriers, shippers, search engines, and payment processors. DHS supports the efforts of the IPR Center’s ECWG and recommends the formation of the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION). Specific ACTION efforts will include the following: Sharing information within the ACTION framework on sellers, shippers, and other third party intermediaries involved in trafficking in counterfeit and pirated goods...”⁴²

EUROPEAN UNION

“To facilitate legal actions and investigations into the sale of Counterfeit Goods, Internet Platforms commit to disclose, upon request, relevant information including the identity and contact details of alleged infringers and their user names insofar as permitted by applicable data protection laws.”⁴³

“Internet Platforms commit to share, upon request, information on suspension of repeat infringers on an individual and case-by-case basis with the Rights Owners concerned, in so far as permitted under applicable data protection laws and in accordance with Internet Platform’s data disclosure agreements.”⁴⁴

The U.S. best practices for platforms do not directly reference improved data sharing, however, this same DHS report includes actions for the U.S. government, and one of these key actions is to improve data sharing among stakeholders. In 2017, the IPR Center established the E-Commerce Working Group (ECWG) to facilitate data sharing between stakeholders, including online marketplaces, express delivery companies, and payment processors, to help them identify, monitor, and stop counterfeit sales. In 2020, ECWG members began working on a pilot data sharing program and established the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION), which will oversee and continue the work of ECWG in creating a private-sector data sharing platform.⁴⁵ The pilot program validated the role data sharing plays in fighting counterfeiting, with actionable intelligence such as: discovering cross-platform illicit activity; identifying individuals and businesses concealing themselves by using multiple IP addresses, business names, business addresses, and phone numbers; and targeting sellers in criminal and civil litigation suits for trademark and copyright violations.⁴⁶

The EU best practices also call for platforms and rights holders to exchange data about counterfeits, including to proactively identify counterfeit goods and repeat infringers. The EU’s MoU emphasizes multiple times throughout the text that platforms do not have a general monitoring obligation, that receipt of information does not constitute “actual or implied notice” or “actual or constructive knowledge” (which could suggest liability for platforms) and that platforms can use information they receive from rights holders at their discretion.⁴⁸ Rights holders who sign on to the MoU also commit to only making “good faith” requests for information.⁴⁹

ASSISTING LAW ENFORCEMENT

Both the U.S. and EU best practices direct platforms to engage with law enforcement agencies to fight counterfeit.

UNITED STATES

“Upon discovery that counterfeit or pirated goods have been sold, platforms should conduct a series of ‘post-discovery’ actions to remediate the fraud. These should include...immediate engagement with law enforcement to provide intelligence and to determine further courses of action.”⁴⁹

“Many foreign sellers on third-party marketplaces do not have a financial nexus to the United States, making it difficult to obtain financial information and to subject all parts of the transaction to U.S. law enforcement efforts. Platforms should close this loophole by encouraging all sellers to clear transactions only with banks and payment providers that comply with U.S. law enforcement requests for information and laws related to (relevant to) the financing of counterfeit activity.”⁵⁰

EUROPEAN UNION

“The signatories agree on the importance of supporting the work of law enforcement authorities in the fight against the sale of Counterfeit Goods over the Internet. To this end, Rights Owners and Internet Platforms commit to cooperate and assist law enforcement authorities, where appropriate and in accordance with applicable law, in the investigation of the sale of Counterfeit Good.”⁵¹

U.S. best practices call for platforms to immediately engage with law enforcement after discovering counterfeit activity.⁵² The EU’s MoU commits signatories to working with law enforcement authorities, but it does not list specific actions that platforms should take.⁵³

U.S. best practices also include having platforms require all sellers to use banks and payment providers that comply with U.S. law enforcement requests to ensure that foreign sellers have a financial nexus to the United States and thus are more easily subject to domestic law enforcement.⁵⁴

CONCLUSION

Online marketplaces have expanded consumer choice and convenience but have also introduced new avenues for bad actors to exploit to sell counterfeit goods. Because they connect both buyers and sellers, these platforms are uniquely positioned to help stop counterfeits, especially when rights holders, law enforcement agencies, and other stakeholders work jointly with them to address this problem.

Both the United States and the EU have developed many overlapping best practices for how these platforms can combat counterfeits that have been endorsed by a multitude of representatives from the private sector and government. Policymakers in other countries should look to these agreed upon best practices as a starting point for future discussions on anti-counterfeiting initiatives, especially if they seek to develop similar voluntary agreements or codify these best practices in law. Establishing a unified set of commercially reasonable and technically feasible practices to combat counterfeit goods will streamline compliance across all platforms and create a united front to protect consumers from dangerous and unlawful counterfeit products.

Policymakers in the United States and the EU can also learn from each other from these best practices. In the United States, policymakers should recognize that the EU MoU heavily emphasizes the responsibilities of rights holders to identify and report counterfeit products on various platforms and consider developing best practices in partnership with the private sector for rights holders. In the EU, policymakers should update the MoU to consider new ideas for platforms that have gained traction in recent years in the United States, such as indemnity requirements for foreign sellers and refunds for consumers.

Finally, policymakers should recognize that these best practices show the value of using soft law approaches to address concerns about online harms. Policymakers on both sides of the Atlantic have demonstrated that not only is it possible to bring together stakeholders to work cooperatively on a complex issue, but that these efforts can be highly impactful and have shown positive results. More work is still needed, but these efforts provide a good framework to build upon.

REFERENCES

- 1 “Global Trade in Fakes: A Worrying Threat,” OECD and European Union Intellectual Property Office, June 22, 2021, <https://www.oecd-ilibrary.org/sites/74c81154-en/index.html?itemId=/content/publication/74c81154-en>.
- 2 “Report from the Commission to the European Parliament and the Council on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet,” European Commission, 2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013DC0209>.
- 3 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 4 Ibid.
- 5 Ibid.
- 6 “Signatories of the Memorandum of Understanding (MoU) on the sale of counterfeit goods on the internet,” European Commission, October 7, 2021, <https://ec.europa.eu/docsroom/documents/47395>.
- 7 “Memorandum on Combating Trafficking in Counterfeit and Pirated Goods,” White House, April 3, 2019, <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/>.
- 8 “Combating Trafficking in Counterfeit and Pirated Goods,” Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 9 “Actions by U.S. Immigration and Customs Enforcement, Homeland Security Investigations, and the National IPR Center since the release of the Department of Homeland Security Report Combating Trafficking in Counterfeit and Pirated Goods,” U.S. Immigration and Customs Enforcement, Homeland Security Investigations, National IPR Center, 2021.
- 10 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 11 Ibid.
- 12 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 13 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 14 Ibid.
- 15 Ibid.
- 16 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 17 Ibid.

-
- 18 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
 - 19 Ibid.
 - 20 Ibid.
 - 21 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
 - 22 Ibid.
 - 23 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
 - 24 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
 - 25 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
 - 26 Ibid.
 - 27 Ibid.
 - 28 Ibid.
 - 29 Ibid.
 - 30 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
 - 31 Ibid.
 - 32 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
 - 33 Ibid.
 - 34 Ibid.
 - 35 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
 - 36 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
 - 37 Ibid.
 - 38 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.

-
- 39 Ibid.
- 40 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 41 “E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices,” OECD, December 13, 2021, <https://doi.org/10.1787/40522de9-en>.
- 42 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 43 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 44 Ibid.
- 45 “Actions by U.S. Immigration and Customs Enforcement, Homeland Security Investigations, and the National IPR Center since the release of the Department of Homeland Security Report Combating Trafficking in Counterfeit and Pirated Goods,” U.S. Immigration and Customs Enforcement, Homeland Security Investigations, National IPR Center, 2021.
- 46 Ibid.
- 47 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 48 Ibid.
- 49 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 50 Ibid.
- 51 “Memorandum of understanding on the sale of counterfeit goods on the internet,” European Commission, 2016, <https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native>.
- 52 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
- 53 Ibid.
- 54 “Combatting Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States,” U.S. Department of Homeland Security, January 24, 2020, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.

ABOUT THE AUTHORS

Becca Trate is a policy analyst focusing on innovation in retail at the Center for Data Innovation. Previously, she worked as a communications manager for the National Association of Broadcasters. She holds a B.S. in Journalism from Ohio University.

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the nonprofit, nonpartisan Information Technology and Innovation Foundation (ITIF).

contact: info@datainnovation.org