High Level Risk Forum

Empowering Consumers to Fight Illicit Trade with Mobile Technology

5th OECD Task Force meeting on Countering Illicit Trade

28 - 29 March 2017
OECD Conference Centre

This paper has been provided to the OECD Task Force on Countering Illicit Trade by the Coalition against Illicit Trade (CAIT). The report illustrates the impact and use of digital solutions to counter illicit trade, including a consumer perspective on demand reduction demonstrating the way in which mobile phone technology can be deployed to identify and monitor counterfeits.

Members are invited to comment on the paper by 30 April 2017.

This document is provided by Leonardo Sforza leonardo.sforza@mslgroup.com and Justin Picard justin.picard@scantrust.com

Michael Morantz (Michael.Morantz@oecd.org), +33185556057

JT03411119

Complete document available on OLIS in its original format
This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.
EMPOWERING CONSUMERS TO FIGHT ILLICIT TRADE WITH MOBILE TECHNOLOGY

SUMMARY

1. Digital technologies allow unique identifiers as well as unique traceability information to be attributed to each product in the supply chain. This paper recommends that governments and member countries, companies, and other stakeholders consider the use of digital verification technology among a wider range of technological and digital solutions to counter illicit trade. This paper contends that the use of such technology should be deployed as an important component in strategic toolkit to combat illicit trade, and one can facilitate the engagement of consumers to take their health safety and security into their own hands. The use of digital technology also represents an important tool for the reduction in demand for illicit products. By scanning products identification systems with their mobile phone, allowing them to be informed instantly about product authenticity and traceability. In turn, scans associated with geolocation information allow the inspection authorities to gain more visibility on the supply chain, and be informed in real-time of any potentially illicit activity, such as counterfeiting or contraband. Being informed that the product they intend to acquire or consume are not legitimate, consumers can put a tremendous amount of pressure on the supply chain, forcing it to self-regulate itself and to eliminate sources of illicit trade, even without the direct intervention of legal authorities.

---

1 Extract from the White Paper on Governance and data management for cross-border tracking, tracing and authentication systems to combat illicit trade and counterfeiting, Coalition Against Illicit Trade, 6 December 2016. This business coalition includes the following companies: Aegate, Atos Worldline, ArjoSolutions, Domino, Essentra, FATA Logistic Systems, Fracturecode, Nano4U, Scan Trust and Viditrust. For more information visit http://www.coalitionagainstillicittrade.org/.
INTRODUCTION

2. Manufacturers of almost all mass-produced and high-value niche products have been operating coding systems for several years now with the aim of ensuring traceability and testifying to the authenticity of their product. Existing tracking, tracing and authentication systems (TT&A), and those that emerge from new technological developments, support manufacturers, logistics companies and public authorities across the European Union and globally in the fight against counterfeiting and illicit trade. Their widespread adoption and operational effectiveness is driven by a number of technical, organisational and policy decisions involving both operators and public authorities which can determine the success or the failure of the systems.

3. The considerations developed here are part of a wider collective report prepared by the members of the Coalition Against Illicit Trade which addresses the key barriers to and the enabling conditions for the adoption of innovative solutions. The coalition strives to facilitate the convergence of business and public policy needs on the basis of its experience as a diverse group of IT-based service providers.

Empowering consumers via smartphone technology

4. With their smartphone, consumers can be empowered to make their own judgment as to the authenticity of their goods and be able to control and check properties and the value of what they buy, as counterfeit/authentic, stolen/legitimate, safe/dangerous, expired/usable, (in)appropriate for given dietary requirements.

5. Tracking, tracing and authentication technologies protect the supply chains in numerous industries and have been employed by brand owners, manufacturers and governments to combat smuggling of branded products and for quality control. These technologies enable supply chain partners to record, monitor and secure products as they move through the supply chain, and verify their authenticity.

6. Until a few years ago, most consumers never knew why products - from eggs to medication boxes - carry human and machine-readable codes. It is fair to assume their closest encounter with coding technology was usually checking the dates on the labels under ‘best before’ and ‘use by’ in the supermarket.

7. Things are starting to change for a combination of reasons, one of which is the inescapable presence of the internet in our increasingly networked world. Equally significant are the 2.6 billion smartphones connected to the internet — a figure that is predicted to top 6 billion by 2020. Together, these factors have so transformed the shopping experience that a recent survey by Planet Retail and GS1 UK found that 28% of shoppers would like to use their smartphone in-store to find what they’re looking for, and 24% want to use a barcode scanner app to view more product information.

8. And this is becoming increasingly possible:

- A product that bears a unique identifier, such as a serialized 2D barcode, can be a powerful way to detect counterfeits and inform users about authenticity, even though it is easily copied. Full traceability in the supply chain is not required for this. What is required however are barcodes that can contain non-predictable data (either random or encrypted); the ability for users and consumers to scan the 2D barcode with a standard app and an active monitoring system. For example a counterfeiter might inundate a market with 100,000 fake products, using one valid code from a genuine product to make the copies. If a mere 5% of products are scanned (a much higher percentage can be achieved if users are incentivised to scan or there is an education
campaign), the counterfeit code will be scanned an average of 5,000 times. With an active monitoring system, the presence of counterfeits will be quickly spotted and localized, and the brand owner can quickly inform consumers, “blacklist” the known counterfeits (by sending out an alert), and launch a product recall.

- Some brand owners and document issuers are open to sharing information explaining how to verify whether the product is original or counterfeit, which aspects of the packaging or product to look out for that are typically not well copied by counterfeitters, and so on. Unfortunately, this information is often buried in websites. Users are not aware of it and do not access it at the time where it matters, for example when buying the product. But this information becomes much easier to access if the user can access it by scanning a code on the product.

- One of the long recognised problems of first-level/overt solutions such as hologram or colour-shifting ink is that the average user typically has no idea about whether a security element should be present on the packaging, and even less so about how the security element should be verified. While there has been a quest for security features that are easy and intuitive to verify, the core issue remains. But this long-standing limitation of overt features is overcome by associating them with a unique identifier: when scanning a product, an animation can be shown indicating how to verify the security feature.

- The powerful image processing capabilities of mobile phones and their ever improving optical capabilities, can be used to authenticate secure graphics, digital watermarks, intrinsic features caused by natural randomness, as well as other optical effects. This, in effect, removes the responsibility of the authentication decision from users, as well as the inherent subjectivity of human decisions.

- Other sensory capabilities of mobile phones, such as their ability to read Near-Field Communication (NFC), or other technologies that may emerge.

9. In summary, mobile phone-based product authentication and tracking solutions essentially make authentication more reliable and accessible to a much wider group of people. Non-experts become far more effective in checking authenticity. The system becomes harder to circumvent for counterfeiters and allows for real-time feedback on authenticity, even in the absence of any security element. It could also increase the effectiveness of standard authentication solutions. And new image analysis-based methods allow for a standardized, objective authentication, reducing the responsibility of the operator in the authentication decision.

10. These developments give public authorities a real opportunity to ensure the general public and end users are aware and can sometimes even participate in either the process of authenticating or checking that a particular product has been authenticated.

11. As such, the consumer is no longer reduced to the role of innocent bystander, unwitting victim of illicit trade, but can also take responsibility for the purchase decisions made.

**Public policy considerations**

12. Public authorities and regulators have a critical role to play in supporting the development of relevant technological architectures to guarantee interoperability across different technological platforms, geographies and industry sectors.
13. The selection of relevant technologies for TT&A should be left to the economic operators of the supply chain, in compliance with technical standards agreed by public authorities or international standard setting bodies.

14. The purpose of T&T systems is to monitor product movements and changes in ownership throughout the supply chain. This information can only be provided by economic operators handling distribution and administrative accounting procedures in warehouses.

15. T&T systems should not duplicate, but complement and be compatible with, established systems and procedures. Moreover, a business-friendly system would provide an opportunity to leverage data mining and insights on production, distribution and product life-cycle.

16. “Unique identifiers” are an enabling tool rather than the objective of a T&T system. Meanwhile data carriers become crucial in the context of mass production of goods requiring high speed manufacture, to avoid disruption in the supply chain.

17. A clear distinction should be made between system operation and independent control. The identification and operation of the most appropriate system should remain with manufacturers and other economic operators involved. Beyond the internal checks carried out by the economic operator, independent third-party checks should be conducted by public authorities or by agreed bodies designated or authorised by public authorities.

18. Given the commercial sensitivity and the liability in case of technical failures, stored data should be considered confidential and owned by the manufacturer or brand owner where data is stored locally. Meanwhile, data should be accessible to certified third-parties such as auditors, law enforcement and public authorities only under strict conditions.

19. Any selected standard for Track and Trace or authentication features should be an open specification that allows systems that use a range of familiar and proven technology platforms and solutions. Reliance on one or a small selection of solution suppliers will increase the risk of delays in deploying any selected TT&A system, and its effectiveness.

20. Avoidance of redundant complexity and costs should be built into the design of all track and trace systems from system inception to system management. Such systems must take into account the value of the products they protect, and safeguard a level playing field for operators on which investment in system and operators acts as a discriminatory barrier for SMEs.

21. The constant development of smartphone technology should be leveraged by brand owners to better associate and empower consumers in the fight against illicit trade and counterfeiting.

22. Non-compliance by economic operators should be clearly sanctioned and associated with proportionate penalties as a deterrent against the non-implementation of the statutory requirements in TT&A.

23. In summary, Public authorities at the national and international level, when addressing policy recommendation and statutory requirements, should take the following into consideration:

- Identifying methodological standards for applying TT&A to production-supply chain processes, although these may be product-specific.
- Defining technical standards only for basic elements of the TT&A process.
• Applying defined standards uniformly to the products to be tracked, traced and authenticated.

• Allowing producers and supply chain operators to select the most appropriate technologies to fulfil TT&A standards, that best fit their respective industrial environments.

• Allow outsourcing of the TT&A applications to “certified” third parties.

• Promoting competition and innovation through the establishment of an accreditation/certification mechanism for systems deemed compliant with the regulatory requirements or the internally agreed standards both for the provision of data and technical standards, irrespective of the technology providers.

• Promoting overarching technological architectures, which would enable interoperability across different technological platforms, geographies and industry sectors.

• Assessing and benchmarking the cost effectiveness of optional solutions taking into account the value of the products they “protect” and the industry specific objectives in tracking and tracing.

• Considering the affordability of initial TT&A investment required for every company and operator in a given industry and market sector, with a view to avoid discriminatory entry barriers for companies due to lack of investment capabilities.

The full report is publicly accessible on CAIT’s website and downloadable here: Governance and data management for cross-border tracking, tracing and authentication systems to combat illicit trade and counterfeiting, Coalition Against Illicit Trade, 6 December 2016.