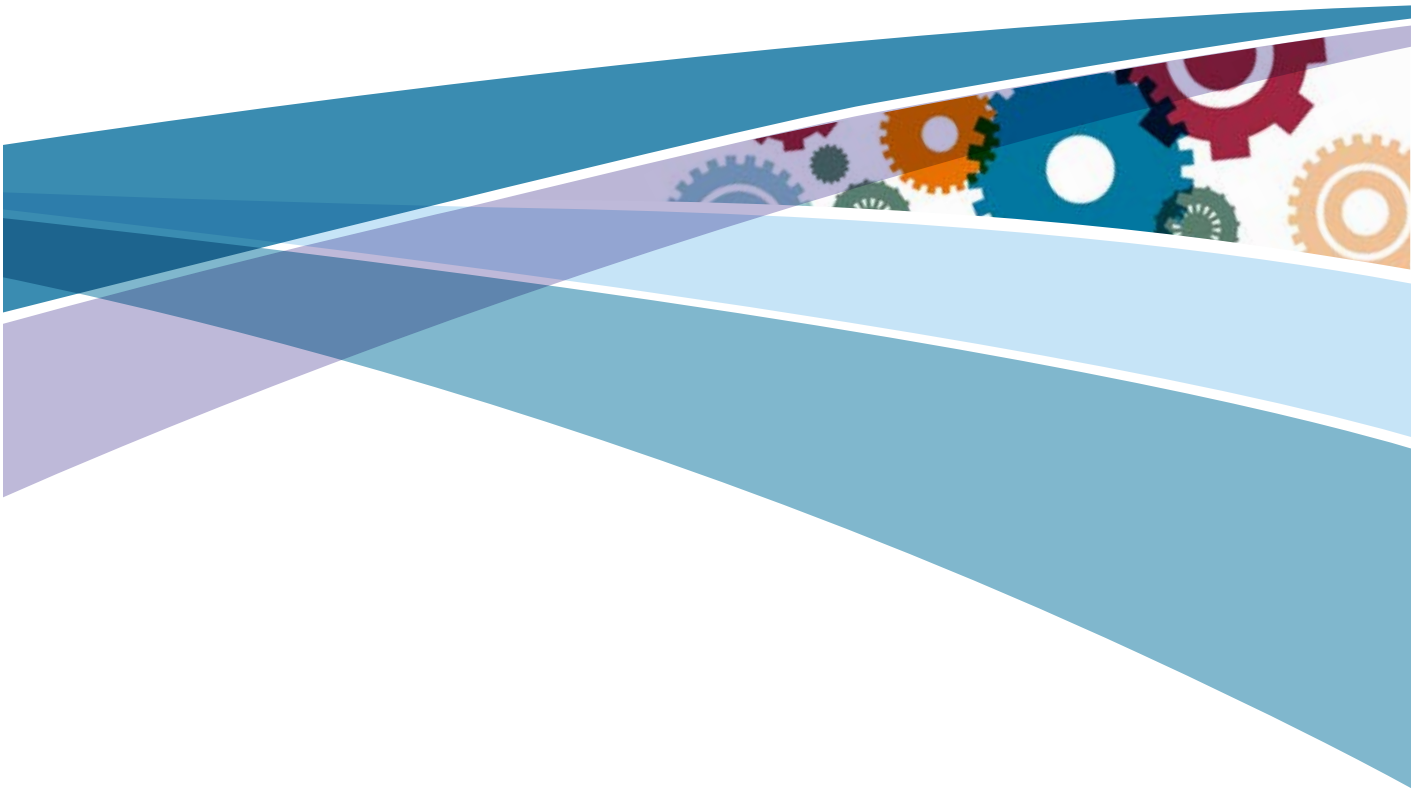
Intellectual Property Office

Share and Share Alike

The Challenges from Social Media for Intellectual Property Rights



Research commissioned by the Intellectual Property Office and carried out by:

Dennis Collopy and Dr. Tim Drye with contributions from Florian Koempel, Peter Jenner and Chris Carey

Submitted version: 20/07/2017

This is an independent report commissioned by the Intellectual Property Office (IPO).
Findings and opinions are those of the researchers, not necessarily the views of the IPO or the Government.

2017/05

A study conducted by a unique team of academic and industry based researchers

UNIVERSITY OF HERTFORDSHIRE

The University of Hertfordshire (UH), the UK's leading business-facing University, is among the most successful new universities in the UK, with a flourishing student community of over 27,700, including more than 2,900 international students from over 85 different countries.

UH's Music and Entertainment Industry Research Group focuses on UK and international creative industries-relevant research.

www.herts.ac.uk/research/ssahri/research-areas/music/meirg

AUDIENCENET

Audiencenet (AN) -a fully accredited market research agency uses state-of-the-art technology to derive deep and meaningful consumer insights.

AudienceNet measures and segments audiences/markets statistically (across territories), then builds bespoke online communities that are a microcosm of the target market.

www.audiencenet.co.uk

ISBN: 978-1-910790-30-4

Share and Share Alike The Challenges from Social Media for Intellectual Property Rights

Published by The Intellectual Property Office
August 2017

1 2 3 4 5 6 7 8 9 10

Any enquiries regarding this publication should be sent to:

The Intellectual Property Office
Concept House
Cardiff Road
Newport
NP10 8QQ

Tel: 0300 300 2000 Fax: 01633 817 777

e-mail: information@ipo.gov.uk

This publication is available from our website at www.ipo.gov.uk

Contents

Executive Summary

1.1 Motivation for the study

The reliance on social media has increased in recent years, with the British Population Survey showing that over 50% of consumers used social media in 2015. Whilst social media has allowed creative content businesses to be able to engage directly with their audience on a commercial and non-commercial basis, there are challenges. Social media provides an avenue and route for would be consumers to be diverted to on-line sites selling infringing content, and evidence from Trading Standards indicates that social media sites were the second most common 'location' for investigations into counterfeiting. It is clear therefore, that the impact of social media on Intellectual Property (IP) has grown, as information and websites on counterfeit goods are accessed and shared; yet there is little, if any, research or dependable data on this issue. Against this backdrop, the Intellectual Property Office (IPO), responsible for supporting and understanding IP Enforcement, has wanted to gain an accurate picture on the impact that social media is having on IP rights holders and consumers of IP.

1.2 Objectives

The main objectives of this research were:

- to assess the role that social media plays in the sale and distribution of counterfeited and pirated physical goods from six representative sectors: alcohol, cigarettes, clothing, footwear, perfume and watches.;
- to estimate recent levels of counterfeiting within the UK;
- to understand the extent to which this is moving online; and
- to gauge how it is helped to do so by online social media platforms.
- The study specifically aimed to assess the scale, impact and characteristics of infringements, as well as opportunities for IP infringement.

1.3 Method

The project was divided into three distinct phases:

Phase 1: Review of literature, government and industry data

This phase involved a review of literature; the collation of recent industry and government seizure statistics; interviews with key representatives from industry and government enforcement agencies; structured surveys with executives from the six key sectors identified as being most impacted by social media; and finally interviews with the three main social media platforms: Google, Twitter and Facebook.

Phase 2: Tracker method and consumer survey

a) Tracker

An online tracker of 12 products, two from six chosen sectors (alcohol, cigarettes, clothing, footwear, perfume and watches), followed links to determine and assess what proportion were directed towards either legitimate or infringing resources. The team designed and developed monitoring tools to locate, track and trace the possible infringement of physical items on Facebook, Twitter and Google.

b) Consumer survey

A 3,000-respondent online survey, complemented by an offline survey focused on the proportion of social media-triggered purchases 'at risk' of being infringing. The survey identified the proportion of those actively engaging with social media; and asked whether their last purchase had been prompted by a recommendation on social media and how confident they were that the purchase was legitimate.

Phase 3: Assessing the harm of purchasing counterfeit products using social media.

The industry surveys were designed to:

- look at the levels of harm from social media-facilitated counterfeiting;
- assess the damage to high and mid-range products;
- examine the direct and indirect damage from counterfeiting to industry, government and consumers; and
- assess the impact of social media and online platforms on the reputations of the brand owners;

As part of this work we also considered the models available for estimating the impact of social media on counterfeiting, particularly in relation to complicit and deceived consumers who typically purchase obvious and non-obvious copies respectively.

1.4 Research Findings

1.4.1 Phase 1 Research Outcomes

The literature review, and responses to our survey questionnaires from industry, government enforcement agencies and technology firms, was focused on assessing the scale, impact and characteristics of infringements, as well as opportunities for IP infringement.

Scale of Infringement

- There were many claims, from industry and government agencies, about the role that social media plays in facilitating IPR infringement. The scale and nature of the infringement was not clear from the responses we received from industry.

- The current scaleable official data is based on seizures. This, combined with the lack of industry data and unverifiable claims, make it difficult to assess the current scale of infringement in general.

- Limited research has been undertaken to assess the scale of infringement and monitor trends, with the key research in this area are the EUIPO's sectoral reports and the OECD-EUIPO report.

- The social media platforms provided data on levels of IPR infringement identified on their platforms in 2015; notably Twitter's data indicated a significant decline in claims for trademark infringement in the second half of 2015, whilst Google argued only a small percentage of 'bad actors' misused their services. Facebook data showed a clear increase in government data requests, although this was not broken down into the types of requests in the research period.

Impact of Infringement

- Industry and enforcement agency responses indicated varying impact across the different sectors, with some firms blaming the rise of social media for an increase in levels of counterfeiting and damage to their business. Despite data from FACT[1], no firm surveyed was able or willing to quantify the actual costs to their business. We attribute this lack of data to industry's reluctance to share confidential financial information. We also recognise that major brands are commercially conflicted in their (often defensive) engagement with social media.

- The main focus for infringement, according to industry and government agencies, is the proliferation of closed groups (i.e. invite-only groups, created on social media platforms). The social media platforms resist enforcement agencies and industry bodies' pressure to adopt more proactive policies for combating infringement. This reactive-only policy towards IPR infringement has created a climate of distrust and suspicion between the platforms and rights holders, something made worse by what industry considers to be the platforms' cumbersome takedown policies.

1 Federation Against Copyright Theft

- The social media firms counter this view by pointing to what in their view is a fragmented UK IPR system, which is part of an even more complex system across 150 other countries.

Characteristics of Infringement

- Despite claims from industry and government agencies about the flagrancy with which IP-infringing content is placed on social media, only one, FACT, provided us with actual examples to highlight the characteristics of infringement.

- Private enforcement agencies detailed how counterfeiters can copy near-identical images from legitimate sites to deceive consumers, pricing these products close to the authentic article. However, such infringing activity takes place across a myriad of online platforms, not just on social media.

- The increasingly sophisticated tactics adopted by counterfeiters in online commerce encompass auction houses, b-2-b marketplaces, social media and, according to some, their link with traffic diversion from official websites.

- We are aware that the use of VPN and the dark net[2] means that much of the current online illicit activity is beyond oversight and reach. On social media platforms, the increased use of spambots and links to various payment sources off-site makes it harder than ever to control the full scope of illicit activity.

Opportunities for IPR

- There was little evidence that social media has been used to promote IPR. However, Microsoft's Bing search engine has shown that online technology platforms can take an active role in combating IP infringement, as shown in their efforts to alert consumers to the dangers of purchasing medicines online, and the likelihood that these could be both fake and dangerous.

- Google's stated zero-tolerance for counterfeits was compelling and there were signs of improved cooperation between eBay and rights holders. Recent changes to Facebook's business model suggest there may be opportunities to improve IP awareness as the firm become more reliant on advertising from the brands whose goods are being infringed within their platforms. Online platforms are most likely to act against illicit activity on their sites if their own business interests (such as advertising) are under threat.

- Education and awareness campaigns to date indicate a need to focus on better informing consumers, in particular around the impact to consumers on their personal safety.

- There is scope for more work and investment by the social media platforms to actively counter IP infringement. In the absence of greater cooperation from industry in supplying data, the focus of future research should be placed on disrupting the current levels of

2 VPN is a virtual private network which uses a public network such as the internet to connect to a private network such as a company's intranet. The dark net is an overlay network that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports - Wikipedia.

consumer complicity. This is an area where social media platforms have a role to play.

1.4.2 Phase 2 Consumer Data Research outcomes

Summary of consumer data

- 17.5% of transactions online were found to be of copied products, and 88% of these transactions were conducted by consumers who knowingly purchased a copied product.
- Social media was the most distinctive medium for communication on copied goods and 24.5% of social grades AB (upper middle class and middle class) acknowledged complicit behaviour, which was significantly more than social grades C (skilled class) where 12.7% acknowledged 'complicit' behaviour.
- Online communication of suspect products was highly concentrated within a very small proportion of participants, particularly located within Facebook:
    - 72.5% of the suspect communications within open groups were generated by 0.78% of promoters.
    - 83.4% of suspect communications within closed groups were generated by 6.2% of promoters.
- Facebook groups represented the most exposed location for suspect communications, with suspect activity being much more prevalent in closed groups:
    - 8.3% of communications within open Facebook groups were found to be suspect.
    - 40.8% (five times more) of communications within closed Facebook groups were found to be suspect.

Scale of infringement

- The survey and tracker indicated that certain goods (like tobacco and alcohol) were less likely to be promoted on social media, but social media can contribute to facilitating infringement.
- We note the high levels of suspect transactions revealed by the tracker, but the data needs to be supported by further regular frequent tracking of online consumer behaviour.
- The scale of infringing activity indicated by the consumer data bears out many industry claims.

Impact of Infringement

- Despite the positives of social media for consumers, the dark side of internet-based commerce is shown by the ease with which both websites and social media pages can be manipulated to deceive consumers. However, our findings, indicate deceived consumers are a small minority of those who use the platforms.

- Closed groups have a strong influence on infringement with complicit consumers five times more likely to shop in closed groups than in open groups.

Characteristics of Infringement

- The bulk (88%) of infringing activity tracked in this study involved complicit consumers.

- The consumer data pointed to deceptive copies as a growing threat, albeit one that still represented a smaller (12%) part of total infringing behaviour on social media.

- Deceptive purchases were more likely to occur with products like clothing, but were not a characteristic of every impacted sector and product, least of all alcohol and tobacco.

1.4.3 Phase 3: Assessing the harm of purchasing counterfeit products using social media

- When assessing the impact of counterfeit products being sold through social media, we have identified that the key stakeholders affected are industry, consumers and government, with the extent of the impact dependent on whether the consumer purchased the counterfeit knowingly or unknowingly. Unfortunately, this study was not able to conduct a full assessment of the harm arising to the key stakeholders, due to the reluctance of industry to share the insight needed. However, from the surveys and research undertaken, it has been able to identify the key challenges facing social media, which can be developed further in future research.

- Industry and enforcement agencies have claimed that low-quality/high-deception goods are likely to be sold on platforms with near-identical, if not cloned, images from authentic goods websites; these are used to deceive the consumer into purchasing them. These may just as easily be offered in open groups, which could add to the sense of authenticity.

- This may also be true of high-quality/high-deception goods, where the pricing may be closer to the authentic price to attract a purchaser looking for an online discount. This is typical of certain products where the reproduction of the goods is near perfect, such as DVD box sets. Equally, the kinds of goods often being disseminated across closed groups seem to be high-quality/low-price products, where damage may be limited.

- The direct and indirect impact on the main three stakeholders – industry, government and consumers – from social media can be assessed as follows, although further work is needed to be able to quantify the impacts:

    - *Direct impact-Loss of industry revenue.*

    Industry have noted a loss of revenue because of the potential substitutional impact of counterfeits on authentic goods, particularly where there is a high degree of deception, although this is lower if the goods are non-deceptive. This represented the most likely impact of social media where the platforms enable the dissemination of deceptive counterfeit goods.

    - *Indirect impact - Reputation harm to industry*

    Reputational harm from the low-quality/high-price goods that are common on social media (according to industry and enforcement agencies).

    - *Indirect impact - loss taxes and the impact on employment*

    There is a widespread evidence that much of the activity emanates from and profits are made by counterfeiters in China and other Southeast Asian markets, causing UK right holders to lose out. There is also the cost to government of having to enforce against IP infringements, such as the activities of Trading Standards.

    - *Indirect impact - welfare benefit for consumers,*

    There may be a welfare benefit (recognised by GAO) for certain types of products (high quality/low price), but for almost all other types of products however the impact is direct.

1.5. Conclusions and recommendations

From the three phases of work we can conclude that;

- Industry groups, together with government and private enforcement agencies, claimed counterfeiting has moved online. This encompasses a complex eco-system involving impersonation, fan pages, social media pages transacting business, promotion and the proliferation of websites selling counterfeits and offering fake special offers.

- According to industry and government sources, social media plays a significant and growing role in the sale and distribution of counterfeited and pirated goods. By providing relative safety within closed groups, as well as the ability to link to off-platform sites for payment, it is easy to see why social media can be regarded as a critical link in the counterfeiting chain.

- However, estimates from government and industry sources on recent levels of counterfeiting within the UK are inadequate and cannot be scaled to reflect the total activity within the market. Our consumer data provides a fresh data point to estimate current levels, albeit only based on a 2015 snapshot.

- Our consumer data reinforces claims made by government enforcement agencies that platforms, such as Facebook, encourage IP infringement and this is particularly flagrant within closed groups. Counterfeiters see social media as a haven and actively use both open and closed group pages, along with 'likes' and 'retweets', to disseminate their offerings. The social media platforms make it easy to move channels by establishing fan pages and making it possible to carry out transactions on or off the social media platform. Social media amplifies counterfeiters' messages by increasing the connectivity of potential complicit consumers. Crucially, these connections do not have to be strong; as the threshold for connection on social media is low.

- Despite the emphasis placed on the threats posed by closed groups, opportunities exist in open groups to secure new users and these represent the greatest threat from social media in amplifying the counterfeiters' messages. Even if the open groups are shut down, they can easily be set up again.

Even though some interesting conclusions have been presented, and the consumer data has shown how social media plays a role in facilitating IPR infringement, particularly in closed groups, the data represents a mere snapshot from the middle of 2015. The lack of any other comparable data means these cannot be used to provide a definitive indication of the development of this phenomenon over time and further work is needed to build upon the work completed in this study. We therefore recommend:

- Improved industry cooperation in supplying essential headline data for government and policy makers to more easily understand the trend in the market. Industry's privileged and confidential information is always a more current and accurate reflection of the market than the data available from government and official sources, which are either out of date or methodologically unsound. This would, in particular, allow far deeper analysis into the harm that purchasing counterfeiting products has on different stakeholders in particular to industry.

- A methodology that allows an assessment of both stated and revealed preferences, such as the one we have employed within this study, would be an effective and reliable measure of illicit activity. The online tracker however, only captured complicit behaviour. To capture deceived behaviour requires an augmented approach, starting with mystery shopping, to identify the relevant links and then track them.

2.0. Background and objectives

2.1 Background

The project's aim was to research the impact of social media on Intellectual Property Rights (IPRs) and specifically to assess the ways in which IPR infringement might be being increased through social media platforms. The research was instigated following claims from government enforcement agencies[3], industry and brands about counterfeiting traffic moving increasingly to online platforms and most notably to social media sites. Given the highly complex nature of social media and the interactions of the millions of users of such services, we decided to start the research process by focusing on physical goods, in the belief that this would yield realistic data that might be useful in subsequent research on digital goods and related phenomena such as user-generated content (UGC).

2.2 Aims and objectives

The primary objective of the research was to compare data and experience from industry, government and consumers to produce a picture of recent levels of counterfeiting within the UK and the extent to which this kind of illicit behaviour is moving online and is being increased through online social media platforms. The study aimed to assess the following four themes:

a) ***Scale of infringement:*** an assessment of the extent to which social media is used to promote IPR, and the extent to which it is enabling infringement and how that infringement is distributed among different sectors, products and types of IP.

b) ***Impact of infringement:*** what are the costs and benefits to IP-intensive businesses of social media, and how has social media changed how IP is used, promoted and enforced? We intended to explore whether IPRs are being applied in new ways or to new types of creative output. A key element was examining the impact on the reputations of creators and IP-intensive businesses and on the health and safety of consumers. The most important part of this segment, in our opinion, was assessing the scale and influence of closed groups (i.e. invite-only groups, created on social media platforms) on IPR infringement.

c) ***Characteristics of infringement:*** we wanted to increase our understanding of where IP-infringing content (closed groups, adverts on social media pages and links to sites/ proxies) was being placed. We also wanted to ascertain the types of infringing products being provided and the formats they are provided in.

d) ***Opportunities for IP:*** the project explored current initiatives used to counter infringement, enforce rights and promote respect for IP, and assessed the effectiveness of these initiatives.

3 Notably in the IP Crime reports 2013-15

Methods used and structure of research

3.1 Methods

The research team applied the methods recommended in our 2014 study 'Measuring Infringement of Intellectual Property Rights', namely collating data from multiple sources, including government and industry and gathering fresh data on consumer attitudes and behaviours.[4] Because of the impact of social media on the distribution and sale of counterfeit goods, we prioritised industry and government seizures and enforcement data along with the results of consumer surveys. We noted one caveat from the 2014 study, namely that in the area of counterfeit and pirated goods there is a highly skewed distribution, particularly of the economic impact of infringement, with a large proportion of the value being concentrated in a very small proportion of the perpetrators. This required a comprehensive study of the infringement enforcement data to identify this tiny segment that escapes sampling methods.

2. Research structure

The research was divided into three phases:

Phase 1: Review of literature and data from government and industry

In this phase we aimed to produce a benchmarked summary of the emerging trends found through a review of literature, a survey of businesses and the collation of recent industry and government seizure statistics. In addition, we wanted to achieve both a top-down and a bottom-up approach to government and industry sources by interviewing key representatives in each sector, by attending industry-led conferences and by visiting the IPO Intelligence Hub which provided a three-year analysis of Trading Standards data. Our initial aim was to find data sources covering at least five to six years to yield a meaningful trend in the data, principally to find out if there has been an appreciable increase in counterfeited and pirated goods being sold as a direct consequence of consumers and retailers moving online.

Initial contact with the Anti-Counterfeiting Group (ACG), Trading Standards and certain rights holders[5] revealed claims that certain social media platforms were producing new offerings ('store' and 'buy and sell') that had the potential to exacerbate the phenomenon under investigation. We initially distinguished between online platforms[6] and social media platforms (such as Facebook and Twitter) because of the different challenges in monitoring the behaviour of buyers and sellers, especially within 'closed groups', given the different technologies involved. This was a key issue with a direct bearing on the methods used for the Phase 2 tasks.

4 'Measuring Infringement Of Intellectual Property Rights – Executive Summary', page 3: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/325020/IP_Measuring_Infringement.pdf
5 Mainly brands impacted by online platforms, e.g. sports goods, clothing, broadcasters' merchandise, perfumes.
6 Here we are mainly referring to Google as the most likely entry point for the discovery of counterfeit or pirated goods.

To provide bottom-up insights alongside the use of top-down government data, we conducted structured surveys with a number of ACG members during the project, focusing on six sectors[7] identified from Google search data, ACG's own information and the official data set[8] as being most affected by counterfeiting. We also aimed to survey the three main technology platforms, Google, Facebook and Twitter, to get their responses to the issues raised by industry and government agencies.

Phase 2: Methods of tracking and the consumer survey

Tracking

For the monitoring process, we tracked six sectors[9], with two products within each chosen sector, using the above methods, as well as using data from the structured business interviews held with organisations from the same sectors. We developed an appropriate system for sampling and, at this stage, tracked a bulk process and then sampled a proportion of the references, in order to follow links to determine the nature of them and what proportion of links were directed towards either legitimate or infringing resources. This enabled us to scale up the sample to the size of the bulk processing. We built the infrastructure, tested it during April 2015 and ran the research tracking over May, June and July 2015, for reporting during August.

Tracker tasks

The team designed and developed monitoring agents to locate, track and trace the possible infringement of physical and digital items (this project focused on the physical products) on Facebook, Twitter and Google.[10] The team also designed a database system to support the monitoring agents and their results, as well as developing a website on which to configure and monitor the agents and review results. Servers were configured to support the system and monitoring agents and an administration system was tested and applied in a production environment. The team had to provide production support, system monitoring and tuning, to review the results, and to extract/organise end-of-project data.

The tasks were: first, to develop and implement the sampling structure for assessing the types of sources promoted via social media and, second, to analyse and estimate the scale of the impact of social media on infringing material. The development, testing and production work was spread over a six-week period. The data captured via the software was available to the IPO under an open licence, together with the algorithms used for the analysis.

7 Alcohol, cigarettes, clothing, footwear, perfume and watches.
8 'IP Crime Reports' for 2014 and 2015.
9 Alcohol, cigarettes, clothing, footwear, perfume and watches.
10 For the sake of clarity, Google is included as the most likely entry point for the discovery of counterfeit or pirated goods.

Consumer survey (3,000 respondents)

The nationally representative survey, targeting 3,000 adults, aged 18 and above, was conducted online over one month (July 2015) and was complemented by an offline survey to fully estimate the scale.

The focus of the survey was on the proportion of social media-triggered purchases which were at risk of being infringing. To find this out involved working from the opposite direction, i.e. tracking the proportion of those actively engaging with social media to look for recommendations and respond to opportunities.

Once we identified the size of this group, we asked them to recall the last purchase they had made that had been prompted by a recommendation on social media and to evaluate how confident they were that the purchase was legitimate. If they claimed to be confident, we asked what methods they used to achieve that confidence, what led them to make the purchase, and how many times they had declined to purchase anything because they thought there was an issue with IPR.

This process involved a series of questions 'funnelling' down to an individual influenced by social media when making purchase decisions, and revealed which social media platforms they used. Then several questions were asked that covered their experience of and level of sensitivity to IPR infringement. We aimed to check whether the purchase was in one of the targeted sectors within the online tracker.

Phase 3: Assessing the harm of purchasing counterfeit products using social media

At the outset, we wanted to understand more fully the expected performance of the products being monitored. This would provide an additional counterfactual position and enhance analysis of product performance versus expectations; we could then compare performance to industry norms or averages. This was, however, not possible on account of the reluctance of industry to share the insight needed. We were also concerned that such an approach could end up repeating the 'forecasting' exercise started by Rand in 2012.[11]

Nonetheless we considered separate interviews with different industry sectors to develop a more nuanced understanding of levels of piracy and counterfeiting around 'hit' and mid-range successful products. We opted eventually to use the industry-structured survey to provide this insight by including questions relating to the scale of IPR infringement and the impact on the brand's market[12]. Even so, the nature of the products chosen for the tracker and consumer survey meant that an accurate assessment of the impact of social media-driven counterfeiting on 'hit' products was too cumbersome a process for those firms who responded.

11 We expressed doubt on whether the Rand Model would meet industry's needs and expectations as described in 'Measuring Infringement Of Intellectual Property Rights', pages 55–57: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/325020/IP_Measuring_Infringement.pdf

12 e.g. "What, if any, economic impact do you consider social media has on your IPR both in terms of infringement and enforcement of your IPR?"

The assessment of the challenges thus relied on understanding the direct and indirect economic harm of counterfeiting on industry, government and consumers and linking this to the role of social media and other online platforms. The assessment provided insights into our research objectives, including the impact of social media on producers' reputations, and identified the characteristics of infringement, such as how certain social media channels are used over others and how particular sectors or goods are targeted. We estimated the impact of social media on levels of purchase of counterfeit and pirated goods by correlating the Phase 2 consumer data on different consumer choices with our analysis of the economic harm from copied products sold in the primary and secondary markets. The primary market is associated with non-obvious copies, where consumers typically purchase a counterfeit product in the belief that it is a genuine product, and where such deceived consumers would want to purchase the genuine product. The secondary market by contrast is linked to obvious copies and is where consumers would purchase a counterfeit product knowingly and willingly; such complicit consumers would be unlikely to purchase the genuine product. Assessing the proportion of copied products sold via social media channels to complicit or deceived consumers from the Phase 2 consumer data is essential for estimating the extent of the economic harm inflicted through social media.

4.0. Research Outcomes Phase 1

Introduction:

We have divided each of the four key research themes into reviews of literature from industry (brands and trade bodies), government, academia and the technology industry, followed by the responses to our survey questionnaires from industry, government enforcement agencies and technology firms. The full responses to our questionnaires have been included in Appendices 1 to 3.

4.1. Scale of infringement

4.1.1. Literature and media review

Industry sources

Bryce and Rutter's (2005) 'Fake Nation'[13] focused on the demand side of counterfeiting, and their report argued that consumption of fakes was commonplace in the UK. Although the authors could not include the impact of the internet at the time, their study influenced part of the design of our consumer survey.

MarkMonitor's (2012) 'Shopping Report'[14] claimed that 20% of bargain-seeking shoppers were deceived into buying fake goods. This is especially relevant to the UK consumer given the much higher level of online purchases in the UK, which are double the European average of 22%. MarkMonitor's more recent 'Global Consumer Shopping Habits Survey' (2015)[15] indicated that 24% of consumers had (willingly or unintentionally) bought a product online that turned out to be a fake.

NetNames' report[16] on the cost of counterfeiting described the "extraordinary" growth of global counterfeiting and, in common with most private enforcement agencies, their assessment relied on official government or industry trade-body estimates.

13 Bryce, J. and Rutter, J. (2005) 'Fake Nation – A Study into Everyday Crime' [Online]: https://www.academia.edu/597794/Fake_Nation_A_Study_into_Everyday_Crime http://webarchive.nationalarchives.gov.uk/20140603093549/http://www.ipo.gov.uk/ipresearch-fake-2005.pdf

14 MarkMonitor (2013) 'Shopping Report 2012' [Online]: https://www.markmonitor.com/download/report/MarkMonitor_Shopping_Report-2012.pdf

15 MarkMonitor (2015) 'Global Consumer Shopping Habits Survey' [Online]: https://www.markmonitor.com/download/report/MarkMonitor_Online_Barometer-2015.pdf

16 NetNames (2015) 'Counting the Cost of Counterfeiting – A NetNames Report' [Online]: https://www.netnames.com/assets/shared/whitepaper/pdf/NetNames-Counterfeiting-Report-A4-2015.pdf

A recent industry study from the US Chamber of Commerce (USCC),[17] cited the headline data from the latest OECD/EUIPO report to highlight their $461 billion estimate of the global counterfeiting market, which is more than double the prior estimate from 2005. The Global Intellectual Property Center (GIPC) for the USCC also released a 'Measuring the Magnitude of Global Counterfeiting'[18] report, which analysed the 38 individual economies that made up 85% of the world's economy. This study claimed that customs authorities were only seizing a tiny fraction of the value of the total estimated counterfeits (as little as 2.5%), and pointed to the 'dearth' of seizure data,[19] arguing that the scale of the global counterfeiting problem has significantly increased, "fuelled by the proliferation of Internet use and social media platforms". The GIPC authors quoted Chaudhry and Zimmerman's assertion that the actual scope of counterfeiting is not "fully known", with current estimates ranging from $200 billion to over $1.7 trillion. These differences are apparently attributable to the varying approaches to counterfeiting adopted by authorities, as well as the paucity of reliable industry data and the diverse methods used to estimate the market. Another illustration of the divergent estimates comes from the 2011 US TV programme Trademark Counterfeiting,[20] which quoted extensively from the International Anti-Counterfeiting Coalition's (IACC) 'Get Real' campaign, citing the "$600 billion per annum" problem. Despite all of the various data sources, including those referred to above, we could find no reliable industry sources that estimated the scale of IPR infringement related directly to social media.

Another, more recent, source[21] highlighted problems allegedly affecting Amazon Marketplace (which accounts for 40% of Amazon's unit sales), which has "morphed into the world's largest flea market" following the firm's efforts to "openly court Chinese manufacturers". These efforts led to sales from Chinese-based sellers more than doubling in 2015, without, according to the report, the installation of the checks needed to cope with the "influx" of counterfeits. The article suggested that the scale of the problem of social media is part of a much greater problem involving wider e-commerce platforms. This confirms claims made by certain private enforcement agencies, like Yellow Brand, about the dangers posed by the largest online marketplaces.

17 Elliot, M. (2016) 'New numbers don't lie: counterfeits pose a growing threat'. *US Chamber of Commerce* [Online]: https://www.uschamber.com/op-ed/new-numbers-don-t-lie-counterfeits-pose-growing-threat
18 GIPC/US Chamber of Commerce (2016) 'Measuring the Magnitude of Global Counterfeiting: Creation of a Contemporary Global Measure of Physical Counterfeiting'.[Online] https://www.uschamber.com/report/measuring-the-magnitude-global-counterfeiting-creation-contemporary-global-measure-physical
19 Ibid., page 4.
20 https://www.youtube.com/watch?v=EnxY0a9Hin8 (25 August 2011)
21 Levy, A. (2016) 'Amazon's Chinese counterfeit problem is getting worse' [Online]: http://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html

Government agencies

International data

Over the past five years, the two most widely used estimates of the global value of the counterfeit goods trade have been BASCAP (2011)[22] and OECD (2009)[23], with the former heavily reliant on the latter. The US Government Accountability Office (GAO) 2010 report [24] noted that several official statistics used in the US were of uncertain provenance and, in the absence of a single official measurement, there was a tendency for global estimates and 'rules of thumb' to be employed when trying to assess overall levels of counterfeiting and piracy. Such estimates ranged between 1.8% (OECD) of legitimate global trade, which was the most frequently quoted measure, and 7% of legitimate global trade (International Chamber of Commerce (ICC)). BASCAP/Frontier [25] argued that the OECD's 2008–2009 estimate only related to international trade and did not include domestically manufactured fakes or digitally pirated goods, the broader economic effects and employment losses. The two other segments of the global market and the associated economic losses were integral to BASCAP's projected estimate of the global value of counterfeiting and piracy as standing between $1.22 trillion and $1.77 trillion. The higher figure is the one most widely cited by industry and the government enforcement community [26].

The US GAO 2010 study[27] identified the different criteria used for almost every sector, which make it almost impossible to arrive at one single figure to accurately measure counterfeiting. The GAO study suggested that this explained the reliance on anecdotal measures and 'rules of thumb', highlighting the difference between the International Trade Council's (ITC) claims that counterfeiting and piracy accounted for 5% to 7% of world trade and the OECD's 2009 estimate of 1.95%.

OECD and EUIPO's recent report, 'Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact',[28] confirmed our concerns about the limited value of seizure data. While confirming the effects of the globalisation of value chains and the rapid growth of e-commerce in enabling the global distribution and sale of counterfeit goods, the authors noted the discrepancies between EU, US and global customs data sets and the rapid growth, between 2011 and 2013, of seized postal shipments across the globe[29] (a result of increased e-commerce). However, the study also argued that the e-commerce market is 'nuanced', dynamic and industry-specific.[30] The report used seizure data estimating that counterfeit and pirated products accounted for $461 billion, or almost 2.5%, of world trade in 2013, but acknowledged that this does not include domestically produced and consumed counterfeit

22 ICC/BASCAP (2011) 'Estimating the global economic and social impacts of counterfeiting and piracy'. February 2011 [Online]: http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study-Full-Report
23 OECD (2009) 'Magnitude of Counterfeiting and Piracy of Tangible Products: An Update' [Online]: http://www.oecd.org/industry/ind/44088872.pdf
24 US General Accounting Office/GAO (2010) 'Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods' [Online]: http://www.gao.gov/products/GAO-10-423
25 ICC/BASCAP (2009) 'The Impact of Counterfeiting on Governments and Consumers' [Online]: http://www.iccwbo.org/advocacy-codes-and-rules/bascap/bascap-research/economic-impacts/
26 WCO at ACG Conference, October 2015.
27 US GAO (2010) 'Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods' [Online]: http://www.gao.gov/products/GAO-10-423
28 OECD and EUIPO (2016) Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. OECD Publishing: Paris. DOI: http://dx.doi.org/10.1787/9789264252653-en
29 Ibid., page 55.
30 Ibid., page 57.

and pirated products.[31] However, there is little here that provides any reliable indication of the scale of social media within this trade.

UK infringement data

The IPO Crime Report,[32] although a highly regarded assessment of counterfeiting and piracy, was still not able to provide a single figure to measure the overall market given the different methods used to assess impact and value. A significant challenge for our study was establishing a meaningful trend from the data made available, as much of what was included was based on snapshots (rather than measurements over time), or methodological issues undermined the data. With that said, the last two versions of the 'IP Crime Report' clearly identified the "growing threat from social media" and indicated that sales of counterfeit goods via social media rose by 15% in 2013–14. Yet the 2015 report also claimed that: "online sale of counterfeit items remains a significant problem […] [but] it has not increased significantly from 2013/14 after a significant increase in recent years". This was a rare example of an estimate of the scale of IPR infringement attributable to social media.

The Trading Standards (National Trading Standards Board) annual survey was a potentially useful metric. Its methodological issues, due to the response rates varying considerably across the survey since its inception, made meaningful comparisons difficult to justify and prevented a clear snapshot of the trend being developed. However, the survey yielded data on the most investigated products, which we were able to compare with Google search terms to support the choice of goods for the consumer survey and tracker parts of this research.

EU infringement data

The European Commission (EC)'s (2009–2014) 'Report on EU customs enforcement of intellectual property rights – Results at the EU border' (2008–2013)[33] provided details on the scale of infringement, breaking down data for each member state and enabling a view of the trend over time. We established that there had been a noticeable recent decline in articles seized (and the domestic retail value of seizures), as well as a tapering-off of cases at the EU border when compared to the period from 1999–2008.

31 Ibid., page 68.
32 IPO (2015) 'IP Crime Report 2015' [Online]: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/461792/ip-crime-report-2014-15.pdf
33 European Commission (2014) 'Report on EU customs enforcement of intellectual property rights – Results at the EU border (2008–2013)' [Online]:http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/2014_ipr_statistics_en.pdf

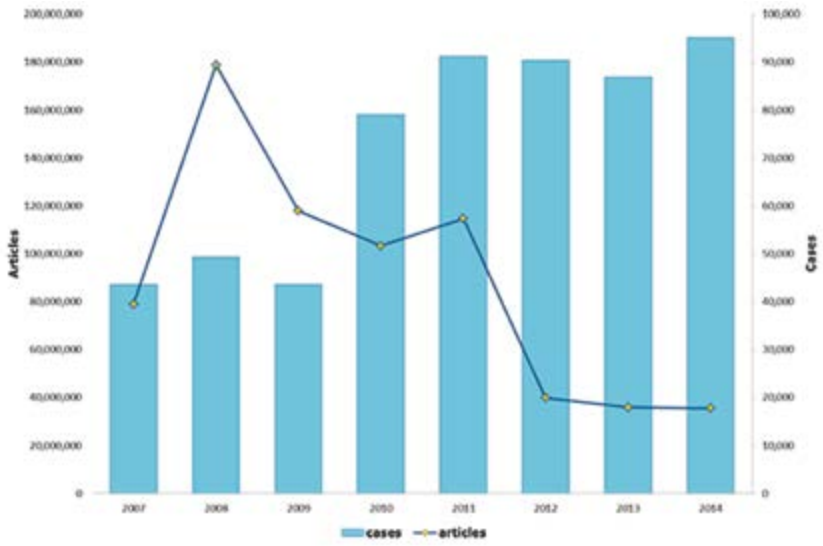


Figure 1: European Commission Data

Figure 1,[34] produced by the EC, clearly shows the decline in the number of articles since 2007 and the stable number of cases (i.e. customs interventions). The decline in articles may have been a result of better enforcement, especially given increased cooperation between rights holders and customs authorities over the past 10 years. It is just as likely that it could reflect changes in counterfeiting traffic, not least an increase in the domestic manufacture of counterfeit goods. Claims that the decline in seizures indicates a drop in counterfeiting traffic are in contrast to assertions made by industry about the rise of illicit online traffic. As such, we believe that the decline in articles seized points to the limitations of customs seizure levels as a reliable indication of the trend.

EUIPO reports assessed the impact of counterfeiting across different sectors and recently formed part of a programme developed with the OECD. We had concerns with the model adopted for several recent case studies (recorded music, cosmetics and clothing) given the reliance on the Rand 2012 method of estimating counterfeits as the difference between actual and forecast sales.[35] The rest of their procedure appeared strong and used innovative approaches to assess the likelihood of counterfeits in different industry sectors. Their segmented approach had much to offer and echoed comments made by the US GAO report, which holds that "effects vary across industries". Developing a data set that could more accurately assess the impact on individual sectors while still using a single process to measure the impact across the industry seems to have considerable merit.

34 European Commission (2015) Taxation and Customs Union - IPR Infringements: Facts and figures http://ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/statistics/index_en.html

35 This was extensively reviewed in our 2013 study 'Measuring Infringement of Intellectual Property Rights', pages 55–56. This may also explain our reluctance to employ this type of model in our economic assessment.

Academic

Bates [36] noted that EU counterfeiting data was limited to details of seizures and pointed to the role of compromised and complex supply chains, as well as the internet, in the fake drugs trade. Naim [37] highlighted the growth rate of the trade in fakes (eight times the rate of legitimate trade since the early 1990s) and how China has become the leading exporter of counterfeits. Chaudhry and Zimmerman's 2009 work The Economics of Counterfeit Trade [38] criticised official data, tracing estimates of the size of the global counterfeit market since the early 1980s to conclude that it was still not clear "what the real magnitude is", noting unclear metrics and data falling short of what was required for policy making. They suggested that the total global counterfeit market had a collective worth of around $500–600 billion, but argued against the use of customs seizures as indicators of counterfeiting levels, claiming that such proxies represent (at best) a tiny fraction of illicit activity. Such flaws in the supply-side data led Chaudhry et al. to call for more demand-side research, yet there is a paucity of such research, with most of the extant work reliant on convenience samples of consumers within single-country markets and few empirical studies being conducted across country markets.[39] The kind of demand-focused research they envisaged would involve investigation of consumer behaviour to understand more easily what motivates people to purchase illicit goods (beyond the incentive of a low price).

Academic research on counterfeiting trends carried out at Michigan State University A-CAPP (Center for Anti-Counterfeiting and Product Protection) included papers by Wilson and Sullivan[40] that highlighted the complexity of counterfeiting and the methodological shortcomings of both government and industry estimates. These also [41] featured comments from brands about the problems of measurement and issues with identifying the number of counterfeits. This was much harder for firms "with sectors across different parts of the supply chain" and was particularly difficult for multinational companies. Elsewhere,[42] the same authors stated that while product counterfeiting "is a global problem that is a growing concern for consumers, government entities, law enforcement, and businesses", current assessments of the nature and extent of the problem are generally unreliable and use processes with significant limitations.

Technology literature sources showing reach of social media

Social media is perceived as the dominant feature of the online world according to research showing 3.17 billion internet users and 2.3 billion active social media users within 2015's global population of 7.3 billion42. Most (91%) retail brands use two or more social media channels while internet users have an average of 5.54 social media accounts each. Those aged 55-64 were more than twice as engaged with branded content than the 28 or younger

36 Bate, R. (2008) *Making a Killing: The Deadly implications of the Counterfeit Drug Trade.* AEI Press.
37 Naim, M. (2005) *Illicit: how smugglers, traffickers and copycats are hijacking the global economy*. IDB Cultural Centre, Anchor/Random Books.
38 Chaudhry, P.E. and Zimmerman, A. (2009) *The Economics of Counterfeit Trade: Governments, Consumers, Pirates and Intellectual Property Rights.* Springer Verlag: Berlin.
39 This was, of course, before the more recent OHIM and EC studies on IP rights perceptions.
40 Wilson, J. and Sullivan, B. (2016) 'Brand owner approaches to assessing the risk of product counterfeiting'. *Journal of Brand Management*, May 2016, Volume 23, Issue 3, pages 327–344.
41 Wilson, J. and Sullivan, B. (2016) *Measuring Product Counterfeiting: Insights from Current Research and Practice.* Michigan State University A-CAPP (Center for Anti-counterfeiting and Product Protection).
42 Wilson, J., Sullivan, B. and Hollis, M. (2016) 'Measuring the "Unmeasurable": Approaches to Assessing the Nature and Extent of Product Counterfeiting'. *International Criminal Justice Review.* 1057567716644766.

age group. The 25–34 demographic was most likely to use Facebook and was the most engaged set of social media users. Ofcom's April 2013 report titled 'Adults Media Literacy'[43] identified significant traits, such as on-going smartphone growth and older users driving the increase in social networking. The regular use of social networking sites was higher in younger age groups (such as 16–24), but in terms of socioeconomic categories those in classes DE and C1 were more frequent users than those in classes AB and C2.

With somewhere between 30 and 33 million users in the UK, Facebook remained the default social networking site for almost all (96%) of the UK adults online.[44] Facebook now includes WhatsApp (1 billion users), Instagram, Messenger (900 million users) and Groups; as such, it now runs four of the six biggest social media platforms. Instagram's typical user profile was 90% under 35 years old, and it was the favourite platform of 32% of US teens.[45] Facebook, in common with Google, has received an increasing number of requests for users' personal data; according to Titcomb,[46] such requests were up by 60% in the UK, with the social network fielding 3,384 demands in six months in 2015 from government and law-enforcement authorities. Facebook[47] claimed to have received more government requests from the UK than from any other countries besides the US and India, and complied with 78% of requests.

4.1.2. Industry and trade bodies' responses

An appeal at the ACG's road shows for 'real' rather than anecdotal evidence demonstrated a fundamental problem facing the various sectors and brands, namely the lack of good, current data to illustrate the scale of IPR infringements. The ACG aimed to collate brands' confidential counterfeiting information to share with government agencies, and it reaffirmed a major challenge for our study in accessing this kind of industry-specific data. Entertainment industry enforcement agency FACT informed us that their current main focus was on dealing with online digital piracy, even though they were still active in the physical goods market, which they described as increasingly less active. Uniquely among ACG member responses, one firm claimed that social media accounted for around a fifth of all their IPR infringement. We gained some insight from various presentations from private enforcement agencies, including NetNames, which claimed that one in every five websites is fake and as many as 40,000 websites were compromised every week. According to them, this meant that, on average, at least 20% of a brand's online traffic could be diverted away from its websites. NetNames also claimed that one in every six products sold online was counterfeit and 30% of EU counterfeit seizures were linked to internet distribution channels. China expert, Yellow Brand Protection, claimed that the counterfeiting industry accounted for 8% of China's GDP. Apart from Alibaba, there are a number of Chinese sites, such as Makepolo, with global reach. Online marketplaces were apparently the No1 online sales channels, with more than 700 active online marketplaces on the internet and 150 in China alone. However, none of these agencies gave

43 43 Ofcom (2013) 'Adult Media Literacy' [Online]: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf
44 McGrory, R. (2015) 'Social Media Statistics for 2015'. *Social Media ltd* [Online]: http://www.rosemcgrory.co.uk/2015/01/06/uk-social-media-statistics-for-2015/
45 Abutaleb, Y. and Maan, L. (2015) 'Facebook revenue, profit beat forecasts; shares hit all-time high'. *Reuters* [Online]: http://www.reuters.com/article/2015/11/05/us-facebook-results-idUSKCN0ST2VF20151105
46 James Titcomb (2015) 'Facebook "snooping" requests increase 60 per cent in UK'. *Telegraph,* 11 November 2015 [Online]: http://www.telegraph.co.uk/technology/facebook/11989781/Facebook-snooping-requests-increase-60-per-cent-in-UK.html
47 Facebook (2016) 'UK Government Requests for Data' [Online]: https://govtrequests.facebook.com/country/United%20Kingdom/

specific data on the scale of social media's role within the fakes market. Their focus appeared to be on the wider issues of traffic diversion and website impersonation, where social media is just one aspect of a wider problem.

4.1.3. Government agency responses

The data available from HM Revenue and Customs (HMRC) illustrated the limitations of relying on seizures. Despite cooperation with industry and other agencies, HMRC had a 'hit' rate of 6% on IPR-related consignments and over 50% of these contained misleading goods. The targeting of large-scale shipments also suggests that they have not been able to deal with the shifting pattern of delivery of counterfeit goods in small packages, evident from the EU border results between 2008 and 2014. Our efforts to review the long-term trends from the various 'IP Crime Reports' indicated that data was not always comparable and the IPO Intelligence Hub confirmed that the data set was unlikely to improve in the absence of statutory reporting on IP crime. According to the enforcement agencies, rights holders and Trading Standards members had complained about the frequency of sales of counterfeit goods on social media sites.

Trading Standards acknowledged the problem of accurately measuring the scale of online illicit activity, not least due to disparate recording of data and intelligence. The situation is made worse by the significant under-reporting of illicit activity (only 5–10%), meaning anecdotal evidence still dominated. They relied on data from the Citizens' Advice Bureau,[48] who handled complaints on 'scams' (including counterfeit goods), and passed on IPR-relevant cases to Trading Standards. The current data showed they have seen a marked increase in the scale of infringement on social media. Since 2010, there has been a 400% increase in complaints attributable to Facebook. Recent data from one region indicated that social media-related IPR infringements far exceeded those of the sale of infringing products on eBay. Intelligence data available via Trading Standards suggested that the sale of physical goods was a dominant factor on social media, with clothing, fashion accessories and DVDs forming the largest categories, accounting for approximately 60% of counterfeit sales. The remaining 40% was made up of footwear, electrical products, toys, toiletries and computer software.

4.1.4. Tech firm responses

Google argued that only a small percentage of 'bad actors' misused legitimate online services to try to sell counterfeit goods. Google's assertion about the low levels of complaints (a small fraction of 1% of advertisers in the past year) was a bold claim and one that called for a response from industry and enforcement agencies. At face value, it suggested that counterfeiting is not as big an issue for search engines as it might be for social media platforms. Twitter referred us to their 'Transparency Report', which details the number of requests received by them from government agencies, as well as industry IPR infringement notices. Their 'Transparency Report' on trademark notices for the six months ending 30 June 2015,[49] and also December 2015,[50] indicated that a relatively low proportion (6–11%) of

48 Facebook is now second only to eBay in consumer complaints to CA, with trends suggesting that Facebook will soon overtake eBay.

49 Twitter (2015) 'Trademark Transparency Report'. June 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jan-jun

50 Twitter (2016) 'Trademark Transparency Report'. December 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jul-dec

accounts had been affected by alleged trademark violations. They noted in the most recent report that the number of trademark notices received for Twitter and Vine had, in fact, declined by 33% (8,588 versus the 12,911 in the previous January–June 2015 report).

4.2. Impact of Infringement

4.2.1 Literature and media review

Industry

The focus of much of the industry literature was on harm to brand integrity and reputation. According to the ACG's Fighting the Good Fight Report,[51] if the products were poor or substandard, consumers were likely to "blame the brand", a description echoed among much of the literature and industry sources. NetNames' recent report,[52] highlighting the cost of the "extraordinary" growth of global counterfeiting, noted that the pharmaceutical sector was most affected. GIPC described the negative economic effects on "consumers, trademark owners, companies […] and retailers, as well as the economy at large". The impact of the lower quality 'fake' goods was to undermine brand integrity, reduce revenue, decrease market share, dilute and damage the brand, and require financial investment to cover the costs involved in enforcing their IPR.[53] Another concern, voiced by MarkMonitor, was that the free speech environment online allowed for negative experiences to affect brands. The damage and harm from these sites came especially from fake special offers that spread very quickly and were not easily identified.

Government agencies

The US GAO's 2010 study[54] criticised all existing and widely used estimates of economic losses that cannot be substantiated, and questioned the assumptions used for substitution rates for fake, as opposed to legal, goods. Their report pointed to the broad range of effects on consumers, industry, government and the economy, arguing that the potential direct effects varied, with those on consumers being both negative and positive, whereas for industry the effect was mainly negative and the effects on government and the economy were entirely negative. The lack of data hindered efforts to quantify the economic impact of counterfeiting and piracy and this resulted in the use of assumptions to compensate, with most estimates being highly sensitive to the assumptions used (including the substitution rate, the value of fakes and the level of deception). The last factor is of real significance to our study as it highlights the fight against counterfeits, which involves very different types of quality and levels of deception and impact, both on consumers and industry. The GAO claimed that no single approach could be used to quantify impact.

---

51 Lewis, P. (2015) 'Anti-Counterfeiting Group: fighting the good fight'. *Trademarks and Brands Online* [Online]: http://www.trademarksandbrandsonline.com/article/anti-counterfeiting-group-fighting-the-good-fight

52 NetNames (2015) 'Counting the Cost of Counterfeiting – A NetNames Report' [Online]: http://www.netnames.com/blog/wp-content/uploads/2015/10/NetNames-Counterfeiting-Report-2015_REVISEDFINAL.pdf

53 GIPC/US Chamber of Commerce (2016) 'Measuring the Magnitude of Global Counterfeiting: Creation of a Contemporary Global Measure of Physical Counterfeiting'. Page 10.

54 US GAO (2010) 'Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods' [Online]: http://www.gao.gov/products/GAO-10-423

Impact on EU

An EC assessment in 2011 stated that it was impossible to estimate the impact of IPR infringement or to measure trends because of inadequate data. The main effects of infringement were seen as reduced investment in innovation and jobs, threats to consumer health and safety, serious problems for SMEs and reduced tax revenue. A second report in 2015 identified effects as reduced legitimate sales, tax revenue reduction, lower employment and the cost of enforcement. Another 2015 study reported that infringing goods accounted for 10% of the EU market, leading to €26bn in lost revenue, €17bn in indirect costs and €8bn in lost taxes. A further study, in 2016, on music piracy was inconclusive, referring only to production and giving no estimate of the impact on distribution or retail.

Academic

The most significant academic source for understanding the impact of IPR infringement is Hopkins et al.'s Counterfeiting Exposed,[55] which proposed a 'harm matrix' encompassing four different levels of deception and quality, from high deception/high quality (such as grey goods, which are branded goods sold by unlicensed resellers at a cheaper price) all the way to low deception/low quality (e.g. cheap Rolex watches). It also identified the different ways that counterfeiting affected brands, noting that fake luxury goods were common in seasonal fashion markets. The authors raised the question of what constituted a counterfeit product if the fake goods were made in the same factories as legal offerings, and this raised an important issue for enforcement as to whether resources are best deployed in contesting such 'grey goods' markets or in focusing on those products that are most harmful. In relation to social media offerings, grey goods can involve both high and low deception but are always high quality and as such have a lower impact and level of harm than high-deception/low-quality goods, which appear to be the goods causing the greatest harm to consumers and potentially to industry, given the potential harm to brands' reputations

4.2.2 Industry responses

Among ACG members, the impact on brands of fakes sold on auction sites like Amazon and eBay was clear from the poor customer reviews resulting from bad experiences. There were claims that established brands, notably those that have to take down hundreds of listings a day, suffer the most. Newly launched goods were thought most likely to be affected after a heavy ad campaign for a product launch, which would drive factories to make fakes more quickly. There was a clear sense that the impact of social media was increasing, with claims of platforms acting as shop windows for fakes, with Facebook in particular a favourite for counterfeit sellers. None of the firms surveyed were able to articulate the economic damage sustained from social media in relation to their IPR, regardless of how critical they had been of the social media platforms. The IP Crime Group's Social Media Group discerned certain online behavioural changes, with one of these indicating that those buying counterfeits were not able (to afford) to buy the 'real thing'; this is an issue we picked up on in the consumer tracker as typical of complicit consumers, whose purchases are of lower economic harm.

55 Hopkins, D.M., Kontik, L.T. and Turnage, M.T. (2003) *Counterfeiting Exposed – Protecting Your Brand and Customers*. John Wiley & Sons.

4.3. Characteristics of Infringement

4.3.1 Literature and media review

The amount of information gathered from a literature and media review on the characteristics of infringement on social media was limited. However, a survey of the main points shows the following:

Industry

According to a report by P. Lewis of the ACG, [56] UK consumers were the most regular online shoppers in the EU, but the market was distorted by the change of distribution practices and by the impact of social media, where photos of genuine goods were used alongside high-quality fake labels and packaging. These methods, combined with prices close to those of the real products, were all used to deceive consumers. The market has seen a further shift in consumer buying habits towards mobile platforms and smartphones, as noted by MarkMonitor,[57] which further enable deceptive purchases.

Examining different consumer behaviours, Spire (2011) [58] divided counterfeits into deceptive, non-deceptive and clones/duplicates, and the types of consumers of counterfeit goods into 'happy purchasers', 'struggling consumers', 'Robin Hoods' and 'innocent purchasers'. Consumer motivation was also central to the conclusions of Bryce and Rutter's (2005) 'Fake Nation'[59], notably that consumers' motives for buying counterfeits were not solely based around economic costs and consumers readily distinguished between different types of products.

Government agencies

The 2011 EC impact assessment [60] cited survey data indicating that many EU citizens have knowingly acquired IPR-infringing goods, with 25% believing it acceptable to buy counterfeits and one in three feeling justified if the price of the legitimate product was too high. The authors noted greater compliance in the UK, Ireland and Denmark than in the rest of the EU. However, OHIM's 2013 'EU Citizens and Intellectual Property'[61] claimed that only 10% of EU citizens openly admitted to IPR infringement but 33% tolerated IPR-infringing behaviours. The report saw a disconnect between support for IPR and personal choices and listed a number of different reasons for this, including limited buying power and protests against the prevailing market economy or premium brands, but concluded that many see IPR as benefiting business elites rather than consumers.

56 Lewis, P. (2015) 'Anti-Counterfeiting Group: fighting the good fight'. Trademarks and Brands Online [Online]: http://www.trademarksandbrandsonline.com/article/anti-counterfeiting-group-fighting-the-good-fight

57 MarkMonitor (2015) 'Global Consumer Shopping Habits Survey' [Online]: https://www.markmonitor.com/download/report/MarkMonitor_Online_Barometer-2015.pdf

58 ACC/Spire Research and Consulting (2011) 'Counterfeits: Measuring it, Fighting It' [Online]: http://www.slideshare.net/spireresearch/010216the-american-chamber-of-commercecounterfeit-measuring-it-fighting-it

59 Bryce, J. and Rutter, J. (2005) 'Fake Nation – A Study into Everyday Crime' [Online]: https://www.academia.edu/597794/Fake_Nation_A_Study_into_Everyday_Crime http://webarchive.nationalarchives.gov.uk/20140603093549/http://www.ipo.gov.uk/ipresearch-fake-2005.pdf

60 European Commission (2011) 'Commission Staff Working Paper: Impact Assessment on Proposal Regarding OHIM and European Observatory on Counterfeiting and Piracy' [Online]: http://ec.europa.eu/internal_market/iprenforcement/docs/observatory/sec_2011_0612_en.pdf

61 OHIM (2013) 'European Citizens and Intellectual Property: Perceptions, Awareness and Behaviour' [Online]: https://oami.europa.eu/ohimportal/documents/11370/80606/IP+perception+study https://oami.europa.eu/ohimportal/en/web/observatory/ip_perception

The EUIPO's 2016 'Intellectual Property and Youth'[62] study researched demand for IPR-infringing goods, using both qualitative research (28 focus groups with respondents aged between 15 and 24 years old) and quantitative research (online survey with 24,295 15–24 year olds from across the EU28). In relation to online purchases of physical goods, clothes and accessories (including footwear) were the most common products. The study claimed that counterfeit goods had a bad image among this age group and found marked differences in young consumers' ability to positively identify websites offering counterfeit goods. Significant differences were detected between markets, with the UK very close to the EU average in most metrics, with only 10% intentionally purchasing counterfeit goods, 12% doing so unintentionally and the remaining 78% either not buying or not knowingly buying.[63]

Academic

Stroppa et al.'s 'Social media and luxury goods counterfeit'[64] study claimed that social media was an important part of the counterfeiting market, enabling illicit transactions off platform via online payment sites. The study identified how brands' investment in Instagram to raise the profile of their products had created a 'promo-friendly environment' that attracted counterfeiters. The methods used by the counterfeiters on Instagram include the use of spambots, which enable them to manage thousands of accounts at the same time, as well as automatic account creation and postings of images that cannot be detected by Instagram's systems.

Stroppa et al. warned that this global trend has grown since their previous research paper, 'Online Advertising Techniques for Counterfeit Goods and Illicit Sales',[65] which focused on counterfeited clothing sold through Facebook-sponsored ads. They argued that creative selling practices, such as those detailed in a 2015 overview by Bloomberg's Roberts,[66] showed counterfeiters targeting the same customers as the authentic brands with high-quality (and comparatively high-priced) deceptive and grey goods rather than focusing on low-price fakes. This is a finding that chimes with claims made by MarkMonitor and NetNames. Stroppa et al. also noted that Google claimed to be cracking down on fraudulent bots that can be costly to advertisers, who pay Google for clicks on their ads. They cite a December 2015 poll, which revealed: "millions of online shoppers are being duped into buying counterfeit products with one in four being ripped-off". Their June 2015 research ('Instagram spam-bots and social media popularity') claimed that Instagram is "infested with millions of spam-bots and fake accounts"[67].

62 European Union Intellectual Property Office (2016) 'Intellectual Property and Youth Scoreboard 2016' [Online]: https://euipo.europa.eu/ohimportal/en/web/observatory/ip-youth-scoreboard?platform=hootsuite

63 These figures are similar to the results of our consumer data (see section 5.5 of the main report)

64 Stroppa, A., di Stefano, D. and Parrella, B. (2016) 'Social media and luxury goods counterfeit: a growing concern for government, industry and consumers worldwide'. [Online]: https://www.washingtonpost.com/blogs/the-switch/files/2016/05/IG_A2016_ST2.pdf?tid=a_inl

65 Their paper was cited extensively in Lepido, D. (2014) 'Fakebook: Site Touts Luxury Goods That May Not Be What They Seem'. *Bloomberg* [Online]: www.bloomberg.com/news/2014-11-13/fake-out-many-luxury-items-advertised-on-facebook-are-phony-researchers-say.html

66 Roberts, A. (2015) 'Luxury Firms Fight Online Fraudsters Over Expensive Fakes'. *Bloomberg* [Online]: http://www.bloomberg.com/news/articles/2015-07-27/fakes-at-7-800-send-luxury-companies-online-to-fight-fraudsters

67 Seetharaman, D. (2015) 'Fake Accounts Still Plague Instagram Despite Purge, Study Finds. Wall Street Journal [Online]: http://blogs.wsj.com/digits/2015/06/30/fake-accounts-still-plague-instagram-despite-purge-study-finds/

Technology industry sources

Facebook's closed groups were the focus of concerns from Chivers[68]; a particular issue was the use of closed and secret groups on Facebook to host online arms bazaars, which is in contravention of Facebook's policies. Facebook's response was to describe their policies as evolutionary, reflecting shifts in their social media ecosystem. They acknowledged that they allowed users to process payments through the Messenger service, as well as providing other features to aid sales.

4.3.2 Industry and trade bodies' responses

China was identified as the origin of most counterfeit manufacture; many products were shipped outside their central distribution network and/or shipped in plain packaging. Clothing and licensed products were most likely to be counterfeited, as was anything in loose packaging. Meeting the problem of counterfeiting required a closed manufacture and distribution network.

FACT noted that technology has changed the physical goods market and social networking websites are now an integral part of modern life, with Facebook increasingly used as an online platform for DVD sales. Social media, together with direct sale websites, online marketplaces and auction websites, is replacing 'traditional' hard goods sales methods. Social media has an influence on almost every type of copyright infringement that FACT investigates, and many 'pirate' websites have Facebook or Twitter accounts. 'Open' groups are used to attract online users and social networking accounts are employed to promote, advertise and directly link to the 'pirate' website. Since the advent of UK website blocking orders, FACT has seen discussions on Facebook of workarounds and suggestions of ways to circumvent blocks. Twitter is used in a similar way, as users tweet and share links to content.

Social media has played a crucial role in assisting IP infringement in the vast majority of FACT's investigations. The use of social media by individuals and groups infringing member content is continually rising and enhancing existing illegal services (hosted on third-party, infringing websites) by keeping users updated with new content and news. Social networking websites are now integral to modern life, and the global reach of the platforms provides the perfect opportunity for criminals to direct the public to infringing content hosted on other websites, to advertise and sell infringing products, and provide on-going 'customer support'. FACT also identified problems with fake/hidden website registration details and overseas servers.

Among the surveyed ACG firms, the key problems in dealing with Facebook resulted from the platform's refusal to close down a 'counterfeiter's' customer profile unless it breached their terms and conditions. There was no clear trend in counterfeiting of new as opposed to old products and purchasers of counterfeits were seen as people seeking 'cheap' products and generally willing to 'delude' themselves into thinking they had got a cheap deal rather than a fake. The key social media-related issue was that "the main sales happen in closed groups, which cannot be scanned easily" and there were problems locating infringing content on

68 Chivers, C.J. (2016) 'Facebook Groups Act as Weapons Bazaars for Militias'. New York Times, 6 April 2016 [Online]: http://www.nytimes.com/2016/04/07/world/middleeast/facebook-weapons-syria-libya-iraq.html?_r=0

social media because of restrictions on Facebook searches. Facebook, and to a much lesser degree Instagram and Twitter, are being used to sell counterfeit products in local selling groups. One respondent claimed that Facebook has taken over from eBay and Gumtree as the major area of concern. Selling pages and closed groups were the main problems for most respondents, even though one saw Amazon and eBay as causing the most damage in the UK. Infringing content was difficult to locate because it appeared in closed selling groups or hidden profiles, unavailable to the average user. Closed groups are often characterised by the use of fake posts and pages, making it harder than ever to catch them without investing a lot of time and resources. What the various ACG members' responses illustrate is the divergence of social media's effects on brands, with some able to identify a clear link to Facebook (and, to a lesser degree, Instagram and Twitter) and the role of closed groups and diversion tactics, whereas others still see eBay and Amazon as the main sources of concern.

There were far more detailed explanations of the characteristics of infringement available from the three main private enforcement agencies. MarkMonitor described the chief online issues impacting brands as impersonation, fan pages, social media pages transacting business, promotion and the proliferation of websites selling counterfeits and offering fake special offers. Counterfeiters see social media as a haven and actively use both open and closed group pages, along with 'likes' and 'retweets', to disseminate their offerings. The social media platforms make it easy to move channels by establishing fan pages and making it possible to carry out transactions on or off the social media platform. MarkMonitor also drew attention to the ease with which counterfeiters could clone brand pages on social media, with some brand-impersonating pages having more likes than the corresponding genuine brand pages.

NetNames described fake web-shops as those with high visibility and traffic that sell counterfeits by using images of authentic brands and logos and working as part of a network. NetNames focused on the whole online, e-commerce landscape, of which social media was just a part. They noted that brand owners were increasingly confronting anonymous online counterfeit and grey market sellers using rogue e-commerce websites and online marketplaces. NetNames saw the B2B marketplaces as the most important, because these were the primary platforms for selling and shipping large volumes of counterfeit and grey market products directly to customers.

They had on-going problems with auction sites, but for them mobile apps were the fastest-growing online channel for counterfeit goods. They also mentioned the dangers of traffic diversion, which involves cyber-squatting and the manipulation of search engine optimisation, as well as the use of social networking sites, blog entries and review sites to divert consumers to rogue e-commerce websites. For NetNames social media was part of a range of online tools used by counterfeiters to divert traffic away from legitimate websites.

Yellow Brand argued that social media channels are increasingly popular targets for counterfeiters, with fake goods being sold on both global and local channels, particularly in China and Russia, as well as via high-volume platforms like Facebook, Twitter and Instagram. Counterfeiters' tactics for avoiding detection include securing content in closed groups. They also had difficulties identifying infringing content such as ads for counterfeits that omit a brand's name and so do not show up in online searches, as well as the dominance of online sales by marketplaces that source stock for many web stores and carry out business in business-to-business and consumer-to-consumer online marketplaces.

4.3.3 Government agency responses

Trading Standards have encountered Facebook-based traders selling counterfeits in 'closed groups' and the 'buy and sell' function for different towns and cities now shows Facebook competing directly with eBay. Trading Standards' greatest concern was the flagrancy of sellers taking photos of their goods 'in situ' and posting them to Facebook who, because of the lack of intelligence and data, simply ignore the problem. Trading Standards also claimed that "sellers enjoy […] ever-greater access to new customers via closed social media groups". They believed that social media was particularly attractive to users when 'advertising' IPR-infringing products because there were no fees or costs yet they were still able to find buyers and sellers in the local area; this made social media an attractive proposition when compared to more traditional online marketplaces such as eBay, Amazon and Gumtree.

IPO's Intelligence Hub described social media as the retail end of counterfeit goods, with Facebook seen as presenting the biggest challenge, since its scale and reach make it impossible to police: enforcement agencies need Regulation of Investigatory Powers Act (RIPA) powers to investigate. It was also claimed that Facebook was not a selling platform, meaning selling goods on the platform could breach their terms and conditions. Social media, it was argued, provided a relatively safe way for members of the public to trade in these goods and the majority of the public in the UK saw counterfeit goods as socially acceptable. Indeed, there were sectors of society that actively sought out counterfeit goods that looked like luxury goods but were more affordable. The public's tolerance of counterfeits, the ease of ordering via the internet, and the relative security of anonymous online entities have created a safe haven for people to trade in counterfeit goods.

4.4. Opportunities for IP

4.4.1 Enforcement activities identified from literature and media review

Industry

Enforcement strategies aimed at purchasers of counterfeits should take account of consumers' greater readiness to listen to victims and experts than authority figures[69]. There is evidence of improving awareness of IPR and increasing consumer knowledge of counterfeits through TV programmes. The BBC's Fake Britain (2014–2015) series stands out, as it explained the danger to consumers as follows: "easily set up dodgy websites and fake identities causing problems – in this case, with life-threatening consequences"[70].

69 ACC/Spire Research and Consulting (2011) 'Counterfeits: Measuring it, Fighting It' [Online]: http://www.slideshare.net/spireresearch/010216the-american-chamber-of-commercecounterfeit-measuring-it-fighting-it

70 BBC (2013) Fake Britain [Online]: https://www.youtube.com/watch?v=-ezrVVtx9uU (16 May 2013)

Government

The National Trading Standards Board (NTSB) in the UK has called for a single agency in the UK to improve IPR enforcement like the creation in the US of a new National Intellectual Property Coordination Center.[71] This initiative brought 23 partner agencies together as a taskforce using the resources, skills and authorities of each partner to provide a comprehensive response to IP theft. The EUIPO's 2016 study Intellectual Property and Youth[72] claimed that arguments relating to personal safety rather than moral values were better suited to convincing young people to think twice about buying counterfeit goods.

Academic

Chaudhry and Zimmerman criticised the current tone of anti-counterfeiting messages and questioned whether firms (and government) actually test their advertisements to assess the influence of such messages on their target audience. Prabhakar[73] argued that online enforcement has been made much harder due to the lack of policing within e-commerce sites and this is made worse by a lack of cooperation and information sharing unless pressed by brands and enforcement agencies. Phillips[74] described the historical problems eBay encountered in dealing with counterfeit goods on their platform and argued that while eBay still has a less-than-perfect takedown system, it is clear that the relationship between certain online platforms and brand owners has improved. In 2005, he also suggested that the UK's Trading Standards was unable to cope with offline counterfeits because of its limited powers and resources; this still seems to be the key problem for enforcement 10 years on.

Technology industry sources

There were concerns about the use of online platforms' terms and conditions, as acceptance of these rarely meant more than a tick-box exercise for users. A more recent UK parliamentary select committee report[75] strongly criticised the length and complexity of the terms and conditions used by social media firms. Even the Electronic Frontier Foundation admitted[76] that the terms are "one-sided in the service provider's favor […] often designed to be beyond any judicial scrutiny […] most users never even bother to read let alone understand these agreements filled as they are with confusing legalese".

Stuart Dredge's analysis of Facebook's Rights Manager tool, their equivalent of YouTube's Content ID system, emphasised its role in managing copyrighted content uploaded to the social network and tackling infringement.[77] This demonstrated the platform's ability to come up with IPR solutions when it was in their business interests to do so. Facebook's sophisticated

71 IPR Center (2016) 'About us' [Online]: https://www.iprcenter.gov/about-us
72 European Union Intellectual Property Office (2016) 'Intellectual Property and Youth Scoreboard 2016' [Online]: https://euipo.europa.eu/ohimportal/en/web/observatory/ip-youth-scoreboard?platform=hootsuite
73 Prabhakar, H. (2012) *Black Market Billions: How organised retail crime funds global terrorists.* Pearson Education Limited.
74 Phillips, T. (2005) Knockoff: The Deadly Trade in Counterfeit Goods. Kogan Page Ltd.
75 Cellan-Jones, R. (2014) 'Social media told to simplify terms and conditions'. BBC News, 28 November 2014: http://www.bbc.co.uk/news/technology-30234789
76 Electronic Frontier Foundation (2016) 'Terms of (Ab)Use' [Online]: https://www.eff.org/issues/terms-of-abuse
77 Dredge, S. (2016) 'Facebook gets its own Content ID with Rights Manager'. *MusicAlly,* 13 April 2016 [Online]: http://musically.com/2016/04/13/facebook-gets-its-own-content-id-with-rights-manager/

technologies, like their DeepText AI,[78] permit the platform; "to sieve through and understand several thousand posts per second across 20 languages" and enable Facebook to 'decode' messages, comments and posts and make recommendations for individual users. This tool could also be employed to search for illicit behaviour.

4.4.2 Industry and trade bodies' responses

The clearest description of ways to bolster enforcement of IPR came from a review of cross-sector best practices by BASCAP's Oldknow, who called for new industry standards, to include the use of automated tools to identify transaction patterns, and the adoption of automation tools, as well as improvement to the transparency of notification, takedown and redress systems. This would require better coordination between intermediaries, government agencies and rights holders, as well as the adoption of preventative tools such as content filtering, verification, track and trace, and the improvement of the security of the global supply chain.

FACT argued that online behaviours demanded a wide variety of methods to deal with infringing websites, such as website closures, detection and removal of infringing content through takedown notices, and the use of auction website listing removal tools. The focus for social media was on reducing illicit websites' popularity through search engine delisting and the removal of the offending pages on Facebook and Twitter, with the ultimate goal of restricting infringing websites' revenues. FACT had a more positive view of the media platforms takedown policies' than we encountered with individual firms, highlighting their procedures with eBay, Twitter and Facebook. The last had an online reporting facility for rights holders and members of the public to report violations, including copyright and trademark issues. FACT had incorporated this procedure into their alternative to a prosecution strategy, with some success. They noted that Facebook would remove specific posts rather than the whole profile or community page, but would occasionally remove entire groups if repeat infringement could be shown.

The ACG member rights holders we surveyed monitored domains and social media online and then took enforcement action against sellers and/or sites selling counterfeit versions of their products or using their imagery. Some used external private enforcement agencies, like MarkMonitor, but others made direct contact with the platforms to lodge complaints. Overall, firms used all the options open to them to enforce their rights online and offline. Some manually collected data from online listings and requested information from marketplaces such as eBay for their records, which they regarded as confidential information, while others relied on their external agents. The perceived resistance from social media platforms involved a time-consuming process of finding, reporting and taking down infringing posts, along with a reliance on images used by sellers in the absence of test purchases. Concerns were expressed about Chinese B2B sites and problems investigating the supply chain, as well as determining the source of the counterfeits. There was less confidence in the current online enforcement process because "criminals are light years ahead of law enforcement" and because of the "high costs of maintaining and enforcing rights" and the "lack of cooperation from online platforms".

78 Facebook (2015) Introducing DeepText: Facebook's text understanding engine https://code.facebook.com/posts/181565595577955/introducing- deeptext-facebook-s-text-understanding-engine/

The IP Crime Group's Social Media Group claimed that social media platforms were not subject to the RIPA 2000 Part III[79] and that any compliance by them with the RIPA was voluntary. They argued that, despite some successes with Facebook taking down pages on sites identified by The Police Intellectual Property Crime Unit (PIPCU), closed groups had become the most challenging aspect of dealing with Facebook, requiring enforcement agencies to go undercover. In their experience, illicit offerings were made across various platforms, with clear links between the social media platforms and online marketplaces. A key insight was the emergence of Twitter as a new threat for digital media rights holders because of the speed with which infringers can publish infringing content, which serves as an illustration of the speed of change within fast-moving markets; even so, there was little sense that Twitter had increased the threat in terms of 'hard' goods.

Facebook's purely voluntary compliance with the RIPA made enforcement hard, as the platform required individual URLs to be forwarded for takedown. This time-consuming and resource-intensive process was the result of the platform's concerns about personal images being included in the takedown and meant that they were unwilling to take down whole albums of photographs. The group pointed to the process where Trading Standards' forensics team monitored fake traders' uploads, but brands were only able to report images impacting their own product. Since not every brand was a member of the ACG, this meant counterfeits of products from non-ACG members could still be offered. At the time, it was assumed that Facebook was not a selling platform, meaning counterfeiters could be in breach of the platform's terms and conditions, which offered an easier tool for disruption than claiming IPR infringements. The main issues for industry were the platform's refusal to accept bulk requests and establishing a more streamlined, coordinated approach to removing infringing content from the platform.

4.4.3 Government agency responses

The existing complex and fragmented[80] enforcement approaches seemed to partly explain the technology firms' current cautious and limited cooperation, but effective IPR enforcement has been further hampered because while the nature of online IPR infringement crime was global, enforcement was local. The apparent lack of integrated approaches meant a need for greater coordination between stakeholders. Only multinational firms could truly adopt a multi-territorial approach, although Europol and Interpol could be part of the solution. Trading Standards issued a call for a single national body for IP crime that could be part of one of the existing agencies (such as immigration, customs or Trading Standards), and this recommendation had real resonance within the UK enforcement environment and chimed with recent changes in IPR enforcement in the US.

The NTSB's and Trading Standards' current 'IP drive' focuses on Facebook and eBay and their national control strategy is about prevention, intelligence and enforcement, although this relies on cooperation with other agencies. Their interactions with Facebook had been difficult given the problems of substantiating the scale of illicit activity and this has remained their biggest challenge in relation to social media. Their reduced and limited resources mean they need more help, especially given the broad scope and scale of their work, with 12,500 feeding investigations, at a time when the local authority Trading Standards model is no longer fit for

79 Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/section/49
80 Seventeen different UK agencies are involved in IPR enforcement.

purpose. Trading Standards proposed a more regional approach as part of the efforts to "join all this up", and this meant being intelligence-led and required greater cooperation from brands, industry bodies and the IPO to tackle IPR infringement on social media. They admitted that their response to IPR infringement on social media platforms had been patchy across the UK and any good practice and active enforcement work was limited in scale. They had encountered problems with identifying the 'owners' of social media profiles, with social media platform operators providing very little (if any) information to enable successful identification and location of offenders. They noted that there was no straightforward mechanism to identify potential IPR infringement on social media, but they had agreed a formal procedure with Facebook after extensive consultation between the NTSB's eCrime Team and Facebook.

The IPO's Intel and Enforcement hub pointed to new initiatives aimed at joining up the current different approaches to reap the benefits of cooperation between industry and IPO/Trading Standards, such as the National Markets group and the Real Deal campaign.

The establishment of the National Trading Standards Board in 2012 was supposed to have created a network of intelligence analysts and a national intelligence hub, but this has not been effective thus far. The current economic climate has resulted in a number of partnerships of necessity, but there has been little coordinated work undertaken in respect of social media due to the stance taken by the NTSB. According to the enforcement agencies, the way the social media groups were constructed required a surveillance authority under the RIPA 2000 to view any infringing goods.

4.4.4 Tech firm responses

Google provided two key documents (How Google fights the advertisement of counterfeit goods and Google's AdWords trademark policies) that set out their stance in relation to AdWords and counterfeited products. There was a clear line in their AdWords policy allowing trademarks to be used as keyword triggers in AdWords, and they claim to be unable to "arbitrate trademark disputes all over the world". Google argued that determining infringement was a matter for the courts, especially as trademarks were territorial and applied to certain goods or services. They said they would, "as a courtesy to brand holders", investigate reasonable claims about trademark violations in their ads and pointed us to their specific region/country policies and their "easy-to-use complaint form". By contrast, Google's stated policy on counterfeits had a very different tone and the firm claimed to have a zero-tolerance policy in relation to the advertisement of counterfeit goods. They claimed that ads on searches for trademarked terms were not confusing as the ads were very clearly delineated as 'sponsored links' and ads that were actually deceptive would violate their Terms of Service. Google argued that the internet had created new complexities and many stakeholders had a role to play in resolving this issue. More significantly, they claimed that brand owners and law enforcement must tackle counterfeiting at its source. However, they also clearly set out the limits of how online services could help given that they "are in no position to determine the authenticity of the millions of advertised goods, as they never even take possession of them, and fraudsters are always coming up with more sophisticated ways to game the system".

Facebook encounter a diverse range of crimes on their platform that affect public safety, but their priorities were whatever affected the safety of consumers, including combating child exploitation and terrorism. Any criminal activity was against their Terms of Service and they were able to 'join the dots' when law enforcement was looking for evidence of criminality. Their real-name policy meant that account holders had to use their full legal name, and this caused the platform problems with enforcement agencies, as they were aware that law enforcement had set up fake accounts, which Facebook could and would close down. In relation to rights holders, they had to accommodate all the various different laws and this required individual notice procedures. Because of this, they were unable to assess bulk processing. That said, they were able to 'whitelist' trade-body reporting for members divided between copyright and trademark infringements, claiming their response turnaround time was within two hours. They had little contact with UK law enforcement apart from Trading Standards and did not encounter many affected stakeholders, but the UK situation was apparently complicated. Facebook's reaction to allegations of infringement was to produce a standard set of questions, as they occasionally received multiple requests. With multi-brand counterfeiters, these were often subject to Proceeds of Crime orders and on-going criminal investigations. There were many existing takedown requests that featured duplicates from rights holders and Trading Standards, usually involving test purchases. Facebook claimed that rights holders could report albums of photos of infringing content.

Facebook is primarily a communication platform, so they are not involved with the online transactions and this is the chief reason for their need to establish the exact nature of any alleged infringement. Facebook had agreements in place with the Home Office and the Information Commissioner's Office (ICO) to meet data requests, including supplying basic subscriber info. This had to come from their Dublin office, although they approved 75% of such data requests. As a US firm subject to US laws on divulging data, it could take six months to get the content of subscriber accounts, although they could volunteer subscriber information if there was a clear justification. They could provide the same information for Instagram where they saw certain levels of infringement. Facebook's lawyers were perceived as risk averse and had difficulties understanding and managing the existing fragmented approach to the enforcement and diversity of stakeholders. Suggested efforts to streamline enforcement that might improve the process still have to satisfy Facebook's requirement for proof. In their formal processes, Facebook claimed, according to their 'Statement of Rights and Responsibilities',[81] that their users were prohibited from posting content that violated another party's IPR. Additionally, they said that they offered tools to report potentially infringing content posted by users on their service. Their online reporting tool could be used to report both copyright and trademark infringements, and they pointed us to the Electronic Frontier Foundation (EFF) 2014 report entitled 'Who has your back?' [82], in which the EFF argues that technology firms need to defend themselves against government requests for data. Apart from acknowledging that law-enforcement agencies could request data relating to a criminal investigation, Facebook only disclosed account records in accordance with its Terms of Service and applicable law. As with both other technology firms, the platform published statistics[83] on government requests for data and content removal.

81 Facebook (2015) 'Statement of Rights and Responsibilities' [Online]: https://www.facebook.com/legal/terms
82 Electronic Frontier Foundation (2014) 'Who has your back? Protecting your speech from copyright and trademark bullies' [Online]: https://www.eff.org/pages/who-has-your-back-copyright-trademark-2014
83 Facebook (2016) 'United Kingdom Requests for Data July–December 2015' [Online]: https://govtrequests.facebook.com/country/United%20Kingdom/

Twitter's specific policy relating to trademark infringement covered anything considered a trademark policy violation and detailed their response to reports of trademark policy violations from holders of federal or international trademark registrations. When satisfied that there was a clear intent to mislead others through the unauthorised use of a trademark, Twitter would suspend the user account and notify the account holder. They distinguished between such accounts and those they determine are accounts that are confusing other users but "not purposefully passing itself off as the trademarked good or service" – in this scenario, they give the account holder an opportunity to clear up any potential confusion. They listed in detail how their counterfeit goods policy prohibited user attempts to pass themselves off as products of the brand owner. They noted how violations could be reported and, if their rules are broken, how such a violation will trigger "appropriate action". Unsurprisingly, they asserted the following: "as is standard industry practice, we do not proactively monitor the content user's post to Twitter".

5.0 Phase 2: Consumer tracker and survey results

5.1 Introduction

The consumer data was based on the results of a three-month online tracker and consumer survey looking at Google/Facebook/Twitter/eBay. The data revealed different types of online consumer behaviour that can be segmented as:

- complicit consumers – actively seek out 'copied' goods
- compliant consumers – avoid copied goods
- deceived consumers – mistake copied goods for the real thing
- unexposed consumers – only find genuine goods

The research team cross-referenced the consumer data with customs seizures data, as these were the most consistent data available relating to the volumes of seizures, even if they were only available for intermittent, very high-level information. The government seizure data showed a jump in reported volumes from 2005–2008 to 2010–2013, but within each group of data the trend was negative. The seizure data generally focused on high-volume opportunities, with each case covered during the initial period (2005–2008) referring to over 2,000 items on average. However, during the second reporting period (2010–2013), the average had declined to just over 270 items.

We focused on six consumer sectors[84], but the specific sector data was only publicly available at an EU-wide level and volumes of seizures differed widely between the different sectors, even though normalised trends indicated that, at the EU level, the trends in seizures were downwards. There are a number of alternative reasons for this including:

- Actual non-compliant behaviour might have been declining within these sectors in line with the overall reduction in seizures in the UK.
- Reductions in seizure activity might have been a result of changes in public policy and/or cuts in enforcement spending. This seemed unlikely as regards the UK, where seizure cases had increased but the average volume of items in a case had dramatically fallen.
- A more likely interpretation was that non-compliant activity had become more diffuse and difficult to detect and capture.

84 Alcohol, cigarettes, clothing, footwear, perfume and watches

- It can also be argued that the distribution of non-compliant products was being handled at a more granular level, which more easily evaded existing government enforcement activity.

Connecting with government and sector-derived statistics

The predominant trends in the available government and industry information are open to several interpretations, notably within individual sectors and official seizure levels. We therefore sought to complement these top-down data sets with bottom-up data. The approach to the latter started from the perspective of purchasing and counterfeiting online, as experienced by individual consumers. We sought to include both explicit experiences, as divulged through a consumer survey, and compare and contrast these with the consumer behaviours captured within the social media tracking study.

Limitations in the approach

In reviewing the current estimates that are based on this bottom-up approach, it is important to keep in mind that there are a number of limitations.

First and foremost, because of the focus on consumer-derived data and the deliberate use of 'naïve' researchers, this study focused on counterfeit goods that, at some stage in the buying cycle, became explicit. In the tracking study, the researchers were not even in a position to assess the actual products delivered by a service, but rather assessed them according to the nature of the online endpoints[85]. Further tracking studies would be required that completed the buying cycle and used detailed expert examination to identify the veracity of the products delivered before this would have a direct link to all counterfeit activity. Furthermore, in the case of the consumer survey, while there was an informal assessment of the products received, this was based upon consumer perceptions, which may well wrongly attribute products. Both options are possible, as properly licensed goods may, on receipt, be erroneously considered substandard or even counterfeit.

Second, this initial investigation was designed as a proof-of-concept 'existence' test, to validate whether these consumer-based approaches could, at viable levels, actually detect significant levels of activity. As such, they were designed to give the activity the best options for detection. This was done by selecting sectors where counterfeiting was, elsewhere, known to be prevalent. Then, within each sector, there was a focus on brands that had high levels of online search activity. This made sense for this stage of a study, but it should be remembered whenever there is an attempt to extrapolate estimates from within the study to more general cases. In this report, the general estimates have been given as a sense of the potential order of magnitude of any impact and also as a demonstration of the types of methods that could be used in further studies, where more wide-ranging sampling methods are deployed.

Third, these initial investigations accepted the challenges involved in building a representative sample of consumers. As we were focusing on online purchase activity, we felt comfortable using online survey methods, and we added some methods of weighting to mitigate any potential for the behavioural characteristics of the study to be preferentially chosen within the

85 namely the sites that facilitate actual transactions

sample. We also sought to design the survey as carefully as possible to reduce response bias. However, none of these effects can be reduced to zero and, at some stage, it may be possible to generate complementary studies via different routes that allow for an unbiased estimate of these side effects.

While there are clear extensions to the current method that can mitigate, to various degrees, the limitations outlined, the most straightforward approach is to introduce a regular sequence of similar studies. This requires a long-term commitment to the approaches but allows the information provided to move from being a snapshot in time, with an ill-defined baseline, to provide a rigorous method that can detect changes. Once stable time series are derived, a series of tools can be used to begin to examine the correlation, lead, lag and impact of different characteristics, in particular, the rise, fall and influence of social media on counterfeiting, as well as assess counterfeiting levels in general. This would be a similar approach to the differences found between the UK national crime survey and those statistics that are linked to police-reported crime.

5.2 Trends in consumers' online behaviour

The longitudinal research on online behaviour conducted by the British Population Survey (BPS)[86] demonstrates a consistent trend of increasing rates of online purchase of non-groceries and alongside it the steady increase in engagement with social media. This is consistent across social grades (Figure 2) and age groups (Figure 3) with anticipated differences between each segment. It is unsurprising that those over 50 lag significantly behind younger groups in the uptake of online purchasing, but it is anticipated that this difference will disappear as those younger groups age. There are obvious financial constraints that explain the difference in purchasing levels between social grades AB and DE[87].

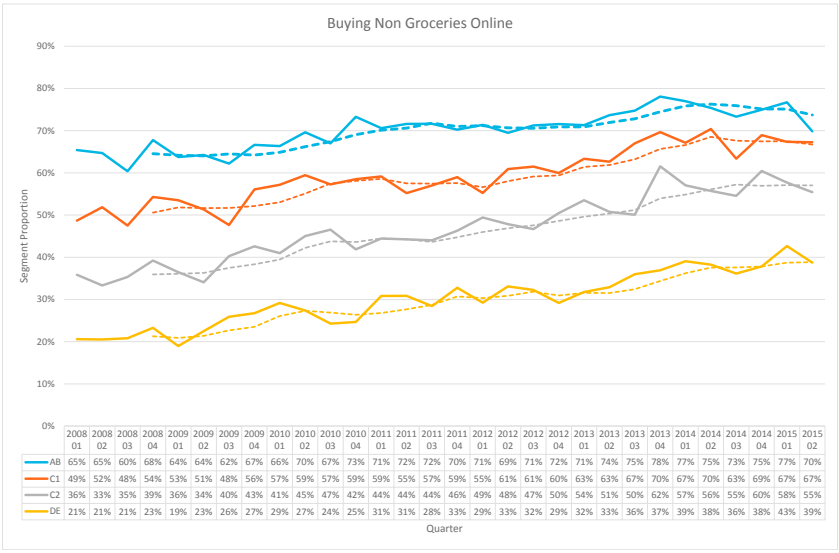
At the same time, as more transactions are being conducted online, there has been an even more dramatic uptake of social media over the years since 2008 (Figures 4 and 5). While the young adopt social media first, at the end of the research period this appeared to have reached a plateau; it is possible that these sectors are moving their behaviour into private messaging services like WhatsApp. There is seen to be much less discrimination in social media use between social grades AB to DE; indeed, social grade C1, by the end of the data, shows the highest amount of use (Figure 4).

The data on trends in consumer behaviour online, demonstrates the plausibility of an increased use of digital transactions that are potentially less amenable to existing methods of enforcement and monitoring of infringement. Furthermore, the BPS has also tracked, since 2010, changes in the claimed influences on buying decisions. The data indicates the overriding influence of both past experience and advice from friends and family. These measures have remained relatively stable throughout the whole research period, with around 70% of consumers claiming that these are influential. In contrast, a small (~5%) but gradually increasing proportion of consumers are being influenced by social media recommendations and also by the presence of brands on social media. It is important to recognise that these are

86 The data has been sourced from BPS' British Consumer Index and is available, for a subscription here: http://www.bcindex.co.uk/channel-trends-special-offer/4584147934 Data can be made available upon request.
87 Social grades AB (managerial and professional) and DE (semi-skilled manual workers and the unemployed)

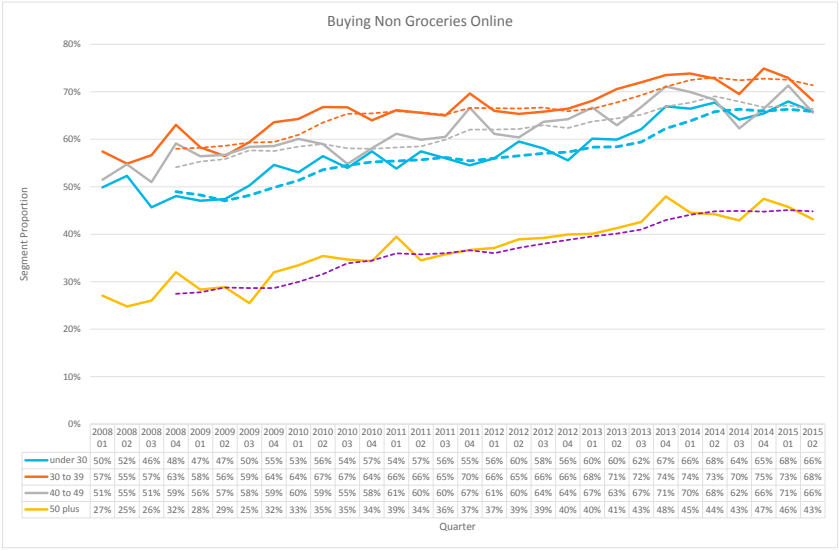
conscious claims, rather than resilient measures of specific influence on research participants, so there is likely to be a level of confirmation bias and wish fulfilment in the responses.

Suffice to say that, at this stage, the trends indicate that should social media have any particular influence on the propagation of financial harm through the promotion of counterfeit products, it is likely to be confined to a relatively small proportion of the population.



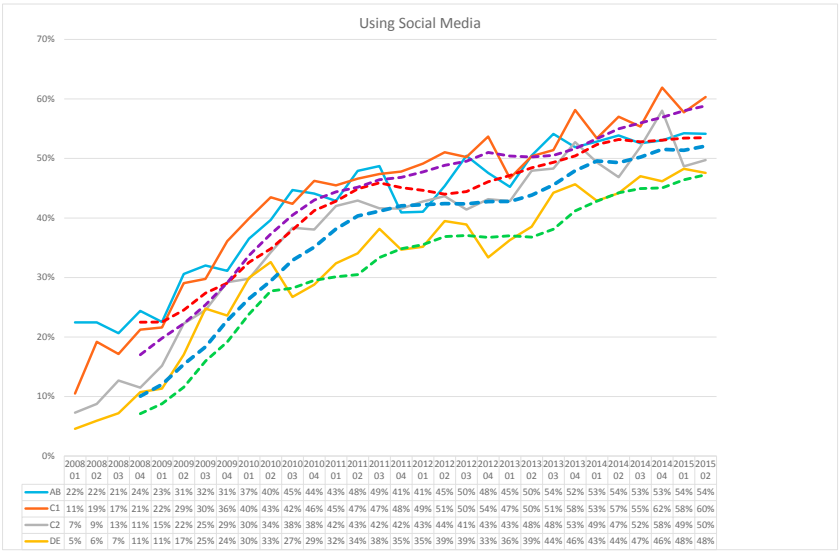
	2008 01	2008 02	2008 03	2008 04	2009 01	2009 02	2009 03	2009 04	2010 01	2010 02	2010 03	2010 04	2011 01	2011 02	2011 03	2011 04	2012 01	2012 02	2012 03	2012 04	2013 01	2013 02	2013 03	2013 04	2014 01	2014 02	2014 03	2014 04	2015 01	2015 02
AB	65%	65%	60%	68%	64%	64%	62%	67%	66%	70%	67%	73%	71%	72%	72%	70%	71%	69%	71%	72%	71%	74%	75%	78%	77%	75%	73%	75%	77%	70%
C1	49%	52%	48%	54%	53%	51%	48%	56%	57%	59%	57%	59%	59%	55%	57%	59%	55%	61%	61%	60%	63%	63%	67%	70%	67%	70%	63%	69%	67%	67%
C2	36%	33%	35%	39%	36%	34%	40%	43%	41%	45%	47%	42%	44%	44%	44%	46%	49%	48%	47%	50%	54%	51%	50%	62%	57%	56%	55%	60%	58%	55%
DE	21%	21%	21%	23%	19%	23%	26%	27%	29%	27%	24%	25%	31%	31%	28%	33%	29%	33%	32%	29%	32%	33%	36%	37%	39%	38%	36%	38%	43%	39%

Figure 2: Long-term trends in consumer online purchasing of non-groceries by social grade
Source: British Population Survey



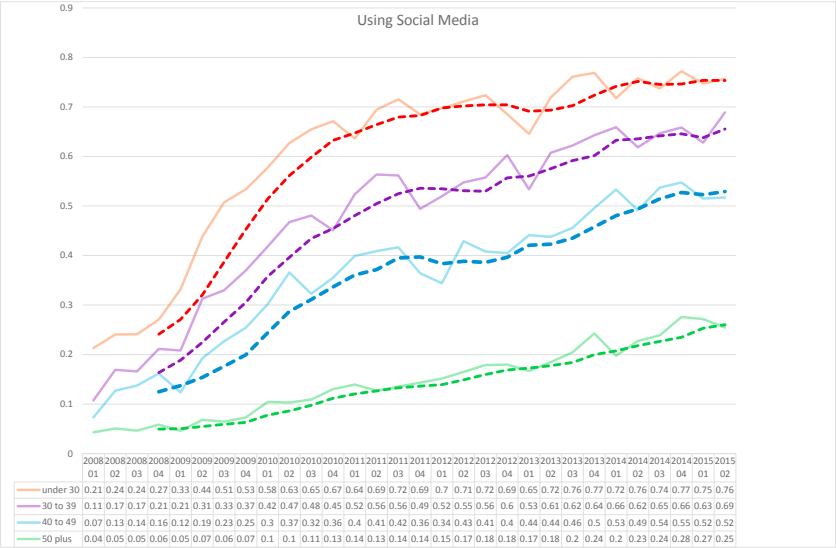
	2008 01	2008 02	2008 03	2008 04	2009 01	2009 02	2009 03	2009 04	2010 01	2010 02	2010 03	2010 04	2011 01	2011 02	2011 03	2011 04	2012 01	2012 02	2012 03	2012 04	2013 01	2013 02	2013 03	2013 04	2014 01	2014 02	2014 03	2014 04	2015 01	2015 02
under 30	50%	52%	46%	48%	47%	47%	50%	55%	53%	56%	54%	57%	54%	57%	56%	55%	56%	60%	58%	56%	60%	60%	62%	67%	66%	68%	64%	65%	68%	66%
30 to 39	57%	55%	57%	63%	58%	56%	59%	64%	64%	67%	67%	64%	66%	66%	65%	70%	66%	65%	66%	66%	68%	71%	72%	74%	74%	73%	70%	75%	73%	68%
40 to 49	51%	55%	51%	59%	56%	57%	58%	59%	60%	59%	55%	58%	61%	60%	60%	67%	61%	60%	64%	64%	67%	63%	67%	71%	70%	68%	62%	66%	71%	66%
50 plus	27%	25%	26%	32%	28%	29%	25%	32%	33%	35%	35%	34%	39%	34%	36%	37%	37%	39%	39%	40%	40%	41%	43%	48%	45%	44%	43%	47%	46%	43%

Figure 3: Long-term trends in consumer online purchasing of non-groceries by age band
Source: British Population Survey



	2008 01	2008 02	2008 03	2008 04	2009 01	2009 02	2009 03	2009 04	2010 01	2010 02	2010 03	2010 04	2011 01	2011 02	2011 03	2011 04	2012 01	2012 02	2012 03	2012 04	2013 01	2013 02	2013 03	2013 04	2014 01	2014 02	2014 03	2014 04	2015 01	2015 02
AB	22%	22%	21%	24%	23%	31%	32%	31%	37%	40%	45%	44%	43%	48%	49%	41%	41%	45%	50%	48%	45%	50%	54%	52%	53%	54%	53%	53%	54%	54%
C1	11%	19%	17%	21%	22%	29%	30%	36%	40%	43%	42%	46%	45%	47%	47%	48%	49%	51%	50%	54%	47%	50%	51%	58%	53%	57%	55%	62%	58%	60%
C2	7%	9%	13%	11%	15%	22%	25%	29%	30%	34%	38%	38%	42%	43%	42%	42%	43%	44%	41%	43%	43%	48%	48%	53%	49%	47%	52%	58%	49%	50%
DE	5%	6%	7%	11%	11%	17%	25%	24%	30%	33%	27%	29%	32%	34%	38%	35%	35%	39%	39%	33%	36%	39%	44%	46%	43%	44%	47%	46%	48%	48%

Figure 4: Long-term trends in consumer use of social media by social grade
Source: British Population Survey



	2008 01	2008 02	2008 03	2008 04	2009 01	2009 02	2009 03	2009 04	2010 01	2010 02	2010 03	2010 04	2011 01	2011 02	2011 03	2011 04	2012 01	2012 02	2012 03	2012 04	2013 01	2013 02	2013 03	2013 04	2014 01	2014 02	2014 03	2014 04	2015 01	2015 02
under 30	0.21	0.24	0.24	0.27	0.33	0.44	0.51	0.53	0.58	0.63	0.65	0.67	0.64	0.69	0.72	0.69	0.7	0.71	0.72	0.69	0.65	0.72	0.76	0.77	0.72	0.76	0.74	0.77	0.75	0.76
30 to 39	0.11	0.17	0.17	0.21	0.21	0.31	0.33	0.37	0.42	0.47	0.48	0.45	0.52	0.56	0.56	0.49	0.52	0.55	0.56	0.6	0.53	0.61	0.62	0.64	0.66	0.62	0.65	0.66	0.63	0.69
40 to 49	0.07	0.13	0.14	0.16	0.12	0.19	0.23	0.25	0.3	0.37	0.32	0.36	0.4	0.41	0.42	0.36	0.34	0.43	0.41	0.4	0.44	0.44	0.46	0.5	0.53	0.49	0.54	0.55	0.52	0.52
50 plus	0.04	0.05	0.05	0.06	0.05	0.07	0.06	0.07	0.1	0.1	0.11	0.13	0.14	0.13	0.14	0.14	0.15	0.17	0.18	0.18	0.17	0.18	0.2	0.24	0.2	0.23	0.24	0.28	0.27	0.25

Figure 5: Long-term trends in consumer use of social media by age band
Source: British Population Survey

5.3. Tracking online promotion of brands

The study aimed to establish the potential relationship between physical goods and social media. It was recognised that a lot of non-compliant behaviour could be attributed to the ease of passing off grey goods (which are branded goods sold by unlicensed resellers at a cheaper price) or near-perfect fakes in online environments. We again segmented the respondents according to their behaviours (i.e. complicit, deceived, compliant and unexposed - see 5.1 above). Definitions for certain key terms used within the following analysis (website end-points, suspect behaviour, communications and Gini curve) are located in Appendix 4.1.

Initially we looked at the levels of exposure to suspect communications, as represented by the four different digital channels we tracked: Google, eBay, Facebook groups (both 'closed' and 'open'), and Twitter. On each of these sources there were initially short lines of text designed to attract interest when a consumer progressed their search for a particular product. We focused our research tracking on six representative sectors: alcohol, cigarettes, clothing, footwear, perfume and watches. Within each sector we tracked two brands, selected on the basis of the levels of search requests as provided by Google Trends in March 2015[88]. This study was initially structured as a proof of concept, as there was little consistent published quantitative material. This made it difficult to extrapolate reliably from the initial results to generate an overall estimate of impact. Instead, the structure was designed to give the maximum opportunity for the detection of interaction effects between social media and counterfeit purchasing. Using these initial estimates further tracking could then be designed. After initial periods of experimental tracking, the study systematically queried the different sectors once an hour over a period of three months, covering June to August 2015. Search

88 We also cross-referenced with Trading Standards data available from the latest 'IP Crime Report', as well as ACG suggestions on key sectors and products.

results were then manually reviewed and characterised based upon the content of the initial return and the destination of any links within the initial result.

Over the three-month period, we reviewed the regular stream of search results. The volume of items is shown in Table 1.

Platform	Captured	Manual Reviewed
Google	5074	5074
eBay	6122	6122
Twitter	39532	726
Facebook (Open)	168174	7835
Facebook (Closed)	3758	512

Table 1: Volume of media items captured and manually reviewed during the social media tracking project

Volumes of search quantities were dependent on the search algorithms within the platforms themselves; it was appropriate to test this as it reflected the experience of the normal users of each platform. The volumes were considerably larger in social media channels like Facebook and Twitter, due to the availability of automated Application Program Interface (API) connections[89]. Due to the highly concentrated nature of suspect behaviour within different social media channels, it was feasible to automate the classification of the links not reviewed manually based upon the risk that these connections were attached to other entities that had already been shown to contain suspect content.

89 An application that can access features or data of another operating system.

Brand	Google	eBay	Twitter	Facebook (Closed)	Facebook (Open)	Total
Chanel	336	393	1135		200	**2064**
Famous Grouse	429	35	61			**525**
Hugo Boss	819	195	3064	1	4	**4083**
Lambert & Butler	235	3	5049(7)			**5287**
Louis Vuitton	464	990	6093		19	**7566**
Marlboro	141	3	15	15	25	**199**
Michael Kors	580	112	7527	17	187	**8423**
Nike	671	1483	11468	249	1504	**15375**
Ralph Loren	217	9	174		24	**424**
Rolex	265	2775	2272		110	**5422**
Smirnoff	446	7	1019			**1472**
UGG	471	117	1655	17	185	**2445**
Other Brands				3459	165916	**169375**
Total	**5074**	**6122**	**39532**	**3758**	**168174**	**222660**

Table 2: Volume of media items captured during the social media tracking project by brand search term

As can be seen in Table 2 the volumes of search results differed considerably across the different search terms. At first sight the data suggested that a greater volume of searches for the products under review took place on Google, eBay and Twitter and that Facebook, while the largest group overall, was actually one of the smallest platforms for these products, possibly indicating it was not used as much for the kind of goods we tracked. In addition, the Facebook closed group volume seemed noticeably smaller, even though this was to prove, as we will see, the source of the most flagrant illicit activity. In fact, this showed that flagrant behaviour only occurred in a very small proportion of the population. This apparent disconnect can be explained because the sampling process within Facebook differed to that used for the other platforms. Within Facebook we had to join a collection of groups, both open and closed, approximately 90 in total, and then capture all the messages within those groups over the tracking period, although we were unable to capture the total reach of these Facebook groups. Therefore, instead of highlighting the discrepancies in volumes between the different platforms, the research focus was on the penetration of suspect activities within each different source.

Google was the most stable platform, as the nature of its content is intentionally less dynamic than other platforms. We can see that the largest group of individual communications was driven by the search terms on Nike within the footwear sector (15,375 searches). Perhaps this reflected the ease of distribution of (relatively small, dry and popular) products by post. By contrast, alcohol had a relatively low presence, was completely undetected within Facebook, and had negligible content within eBay. Smoking promotion was similarly low, perhaps reflecting eBay's terms and conditions of use[90]. The exception to this volume was the results for the brand Lambert & Butler within Twitter; this was likely to be the result of particular public and press interest in a Liverpool football player called Ricky Lambert. Indeed, applying a very strict filter to the results yielded only seven results for the full brand name. Strictly speaking, any promotion of cigarettes is banned within the UK, so all of these promotions would have been suspect and anyone actively seeking these search terms was in some sense complicit. However, for the purpose of this particular study we classified the links according to whether they directed the user towards what looked like genuinely branded locations or other suspect locations.

As already indicated, within the UK any promotion of cigarettes is legally suspect and this is corroborated by the low volumes of links within searches on this brand that resulted in a link to a genuinely branded website. Where the link appeared genuine, the branded content was predominantly hosted by supermarkets, and the cigarette brands themselves appeared to have removed all links. This discrepancy in behaviour was particularly noticeable within the results for Google (Figure 6): suspect links were particularly rare in all instances, other than for Marlboro. The other notable feature was the prevalence of suspect links for Nike footwear within eBay (Figure 7). This stood out in terms of the volume of suspect links but, as will be shown, this particular market in Nike-branded footwear appears to behave idiosyncratically and may have been a transient behaviour during the period of the trial.

90 http://pages.ebay.co.uk/help/policies/tobacco.html "You're not allowed to sell tobacco products on eBay, including collectable packaging that contains tobacco, because of strict government regulations"

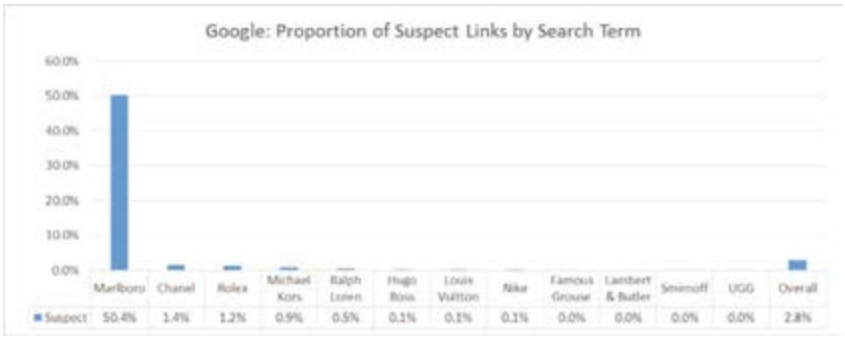


Figure 6: Proportion of suspect links identified within the items tracked from Google

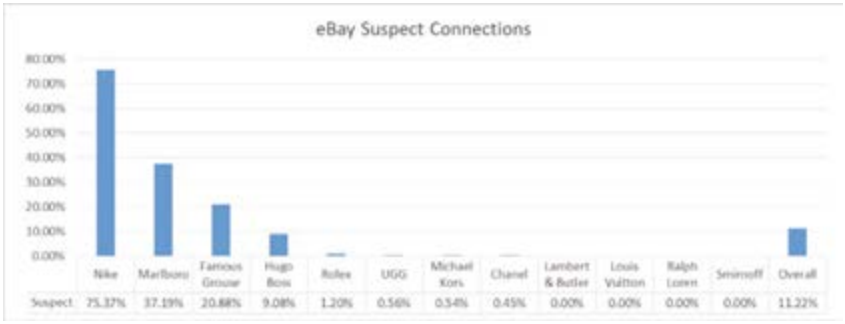


Figure 7: Proportion of suspect links identified within the items tracked from eBay

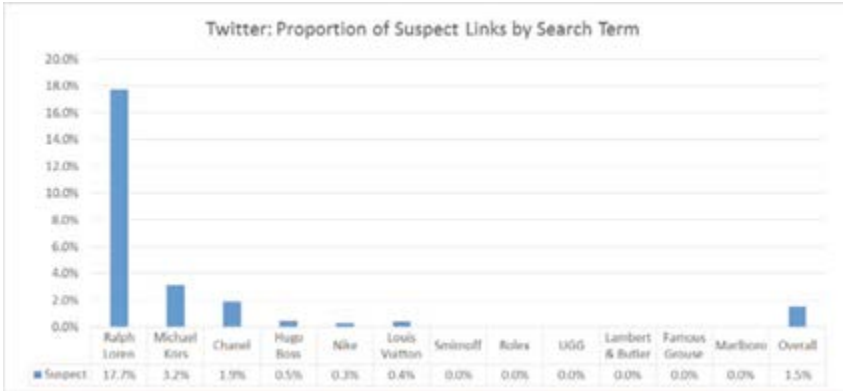
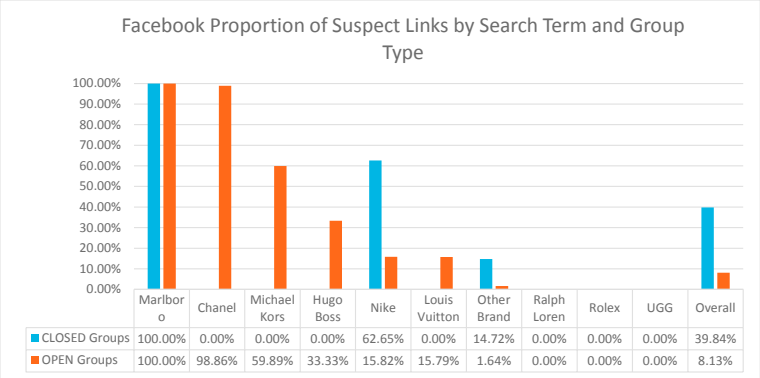


Figure 8: Proportion of suspect links identified within the items tracked from Twitter



	Marlboro	Chanel	Michael Kors	Hugo Boss	Nike	Louis Vuitton	Other Brand	Ralph Loren	Rolex	UGG	Overall
CLOSED Groups	100.00%	0.00%	0.00%	0.00%	62.65%	0.00%	14.72%	0.00%	0.00%	0.00%	39.84%
OPEN Groups	100.00%	98.86%	59.89%	33.33%	15.82%	15.79%	1.64%	0.00%	0.00%	0.00%	8.13%

Figure 9: Proportion of suspect links identified within the items tracked from Facebook groups, open and closed

When reviewing the distribution of the sources of suspect links (Figures 6 to 9), it was clear that different channels attracted attention from different communities of interest as the proportions changed markedly, although we were unable to say how transient this phenomenon was. Given the types of behaviour shown elsewhere in this report, it was likely that this fluctuates widely as various 'herd' characteristics dictate variations. It was also plain to see that the proportion of suspect classifications was much larger within the Facebook platform, within both open and closed groups. However, this may well simply reflect our concentration on popular brand names within each of the consumer sectors. Due to the nature of the API process, and the concentration on Facebook groups, the study was able to capture reference data for additional brands within the groups tracked in the research. This comparison demonstrated that, in this instance, the scale of suspect behaviour outside the target brands was at a significantly lower rate, at suspect link rates of 14.7% and 1.6% within 'closed' groups and 'open' groups respectively. While the overall rate was reduced, the enhanced exposure to suspect material was still high (over 500%) when comparing closed groups to open groups.

Different online entities

Website endpoints

As well as the classification of overall exposure above, it is insightful to delve beneath the surface and characterise the structure of the behaviour behind these top-line figures. It quickly became apparent that a number of different entities were traceable. The first entity relevant to the search was the final endpoint of the information. In each platform, this was:

(a) the live link that is presented within the Google search;

(b) the end of a chain of links within Twitter, which would often begin with a random short code;

(c) the conclusion of a chain of items within Facebook.

The nature of eBay meant it led to minimal external references. In the manually assessed records, these links were followed to an online location that was either available for a product sale or ended in some other non-transactional information (for example, a short review like a blog). Root sites are the hosting part of each address URL, and have been classified as follows:

(a) 'genuine' referred to those root sites that represented a supplier website or a branded distribution site (or the products were pre-owned or found at some other legitimate but non-core source);

(b) 'suspect' where a significant proportion of products were identified by some form of misrepresentation, most often by offering very high discounts (for example, 10–20% of normal pricing);

(c) 'other' is the classification of links that go to known product purchase locations (e.g. information or other branded materials).

Across all the analysis conducted, a total of 1,354 different root sites were identified, and the behaviour within these different endpoints was strikingly different (Figure 10). High proportions of the non-transactional communications self-referenced Facebook and Twitter, amounting to 97.7% of the 'other' classification (Figure 11). Transactional endpoints were dominated by eBay, which was the location of 17.6% of genuine transactions. A small proportion (0.2%) of suspect links appeared to fraudulently make use of website root names that included branded names; these were clearly traps set for the 'deceived'. Further to this, it is seen below that 68.7% of all suspect links were located in just three distinct host web locations.

This was the first indication of the highly skewed nature of the online behaviour. This presented a sampling challenge, and meant that initial volume estimates were subject to high degrees of risk. Over 80% of all three classifications of root types ('genuine', 'suspect' and 'other') occurred within just 114 different locations. On the basis of this structure, it appeared manageable to close down the vast majority of suspect behaviour by blocking a few locations; however, while this type of suspect behaviour was narrowly defined, it was also found to be highly mobile.

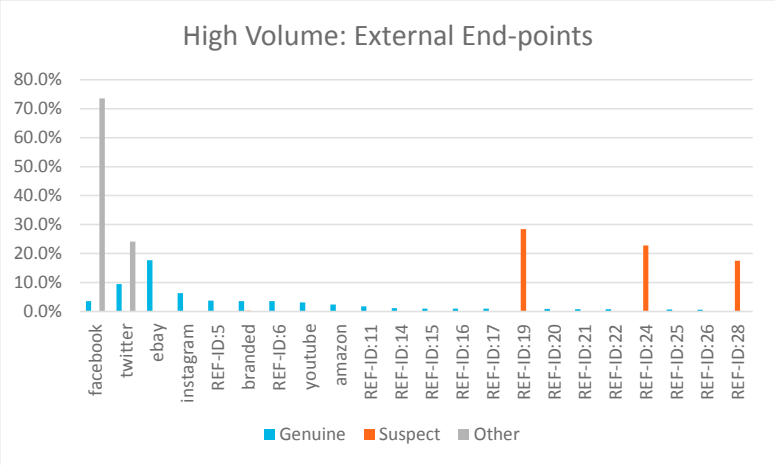


Figure 10: Proportion of End-points by type of link and host

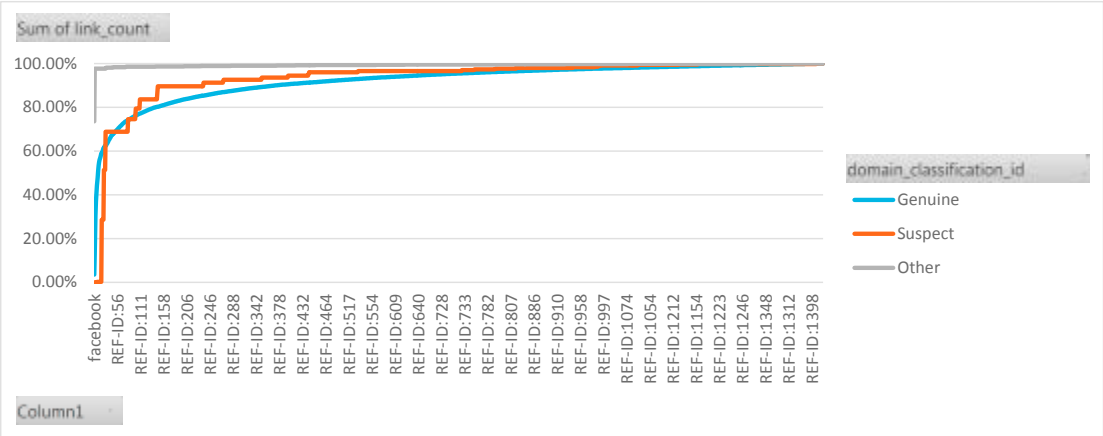


Figure 11: Proportion of suspect links identified within the items tracked from Google

Online initiators

As has been shown, the endpoints for all types of behaviour, in particular suspect behaviour, were highly concentrated. By examining the nature of the links, it was possible to examine the unique origin of behaviour. This can be assessed by tracking the usernames for each type of behaviour. We defined three different properties of information:

1) The first is the initiator – this is the reference that is unique across (potentially) a number of different posts.

2) The second is each individual post – this is a unique communication present in one or more search results.

The third is the post lifetime – this is defined as the length of time between the first search when a particular post was identified and the last search when the same post was recognised.

We then added together the lifetime of each individual-selected post by initiators to generate overall estimates of exposure. With these definitions it was instructive to compare the different behaviours that are shown (Table 3) across the platforms examined.

Social Media Tracking (Overall)	Overall Exposure	Average Number of Posts	Number of Initiators	Average Lifetime (Days)	Average Exposure Length (Days)
Google	120680.1	115.21	2755	0.38	43.8
Twitter	43000.6	9.25	23881	0.19	1.8
eBay	112925	67.89	11950	0.14	9.45
Facebook (Open Groups)	175685	15.63	35267	0.32	4.98
Facebook (Closed Groups)	7746	39.38	537	0.37	14.42

Table 3: Summary statistics, by online platform, for items broadcast

Google clearly showed a more stable setup, with far fewer (2,755) different initiators than the other platforms, which provided a significantly higher number of posts. In this instance, a 'post' describes when a particular linked web location remains identical to those before, based upon a hash of the webpage content, between one search and the next. So, each individual initiator had a presence across nearly half (43.8 days) of the survey period of 92 days. By contrast, Twitter presented a highly dynamic environment, with a substantial number (23,881) of initiators, with a very short average exposure of 1.8 days. The highest level of exposure tracked by the study occurred within open Facebook groups, and this platform contained the highest number (35,267) of initiators; however, these open groups had a relatively short level of exposure (4.98 days).

Social Media Tracking (Overall)	Proportion of Suspect Initiators	Proportion of Suspect Posts	Suspect Exposure
Google	1.90%	2.00%	1.50%
Twitter	0.10%	0.10%	0.30%
eBay	9.90%	2.90%	0.60%
Facebook (Open Groups)	3.90%	8.00%	8.30%
Facebook (Closed Groups)	30.80%	39.80%	40.10%

Table 4: The proportion of suspect initiators and posts by online platform

Comparing the distributions of the suspect behaviour in the table above (Table 4) demonstrated that, while the lowest proportion (0.3%) of suspect behaviour occurred within Twitter, an even smaller proportion (0.1%) of suspect initiators perpetrated this behaviour. Those who appeared to conduct suspect communications were three times more active than the average participant on Twitter. This behaviour contrasted with Google, where suspect sources were less active than average participants, as 1.5% of exposure was linked to 1.9% of initiators. This suppressed behaviour was further replicated within eBay, where a high proportion (9.9%) of suspect initiators only distributed a small proportion (0.6%) of exposure. It is tempting to explain this distribution as a hangover from anecdotal suggestions that eBay used to be the location of much suspect activity, but the platform is now better able to suppress this non-compliant behaviour. In contrast to eBay, within Facebook there was again a tendency for suspect initiators to be more active than other participants, so 8.3% and 40.1% of exposure were delivered by 3.9% and 30.8% of initiators, for closed and open groups respectively. While the uplift in suspect exposure was over 100% within open groups, within closed groups the scope for uplift (~33%) in exposure from suspect initiators was suppressed because the populations of the closed groups were so heavily dominated by this suspect behaviour.

These characteristics suggested very different behaviour between the different platforms, which have been further demonstrated by detailed examination of the distribution of exposure through the use of Gini Curves - see Appendix 4.2. These very different distributions (Table 5) point to quite different approaches to resolving the situation. It is suggestive that this approach is focused on the current ability of individual initiators to inject high volumes of communications into a platform. Google and eBay represent more mature platforms although they have had phases when they were susceptible to various forms of spamming, which previously occurred within email. There have been many attempts to game PageRank[91] algorithms within Google to raise items up Google search results, but these possibilities look to have been successfully suppressed, at least in these searches. The results suggested that eBay is also reaching this level of maturity too. Suspect behaviour appears to be the most straightforward type to intensify within the social media context, with a high volume within Facebook. In particular, over a period of development, non-compliant behaviour could begin to damage reputations; however, sophisticated filtering and detection methods may help to suppress suspect activity.

Social Media Tracking (Overall) 10% of Initiators	Branded	Genuine	Suspect	Other
Google	4.70%	26.70%	2.70%	8.30%
Twitter	98.60%	97.90%	96.40%	88.00%
eBay	64.20%	29.20%	0.00%	53.50%
Facebook (Open Groups)			94.30%	91.50%
Facebook (Closed Groups)			100.00%	98.40%

Table 5: The proportion of exposure within each online platform by content type, from the most prolific 10% of initiators

91 An algorithm used by Google Search to rank websites in their search engine results.

5.4 Consumer survey

Having explored in detail the digital promotion of products, we now turn our attention to the experience of consumers who look to make purchases online. This should complement the perspective provided in the previous section. In conducting this study, we first have to address three challenges: online sampling selection, verification of suspect online personas, and handling the highly skewed nature of typical digital behaviour. The approach that we took to address these challenges has been detailed in Appendix 4.3.

The questionnaire was conducted in July 2015 and 3,000 consumers were interviewed. The data was indicative of a certain type of behaviour in relation to popular brands, and the test was designed to identify the most likely locations for copied products so as to assess the impact of social media. The test was about searches for particular popular brands, rather than being a representation of general online purchasing behaviour. Nonetheless, the data shows a pattern that further surveys and tracked research could build on.

There are further caveats about those who take part in online surveys, as well as the use of the term 'copied' products within the survey, which has a broader scope than 'infringing' or 'fraudulent' products. Even though these findings have to be properly contextualised, it is clear that this data supports many industry and government agencies' claims about the roles that the internet and social media have in enabling counterfeited products to be made available and purchased. We were concerned about the credibility of claims of high levels of complicit behaviour, but the study was designed to focus on areas where complicit behaviour was more likely, giving us the chance to distinguish the specific role of social media. Contrary to our own assumptions before the study, this appeared to be considerable.

The project's aim was to demonstrate, through research, that social media and online sites increased the scale and impact of counterfeiting and piracy. The resulting data indicated how much easier it was to consume and supply fake goods through web-based marketplaces and social media, which is hardly surprising given the impact of social media and the internet on modern life. The counterfeit trade may well be little different from any other activity, but the change this data points to is one of scale. The key results from our consumer survey are:

- 17.5% of transactions online were found to be of copied products:
    - Of this, 15.4% of online transactions were conducted by a 'complicit' segment of consumers who willingly participated.
    - Only 2.1% of online transactions were accidental purchases by individuals who were 'deceived' and only found this out on receipt of the goods.
- Social media was the most distinctive medium for communication on copied goods:
    - 46.1% of 'complicit' purchases involved social media.
    - In contrast, only 4.1% of 'unexposed' purchases involved social media.

- Social grades AB were significantly involved in ‘complicit’ behaviour:
    - 24.5% of social grades AB acknowledged ‘complicit’ behaviour.
    - In contrast, only 12.7% of social grade C2 acknowledged ‘complicit’ behaviour.
- Online communication of suspect products was highly concentrated within a very small proportion of participants, currently particularly located within Facebook:
    - 72.5% of the suspect communications within open groups were generated by 0.78% of promoters.
    - 83.4% of suspect communications within closed groups were generated by 6.2% of promoters.
- Facebook groups represented the most exposed location for suspect communications, with suspect activity being much more prevalent in closed groups:
    - 8.3% of communications within open Facebook groups were found to be suspect.
    - 40.8% (five times more) of communications within closed Facebook groups were found to be suspect.

Overall, these figures made an impact and there are clear implications to be drawn from this data. The 17.5% of transactions online found to be copied products, is almost double the highest modelled estimates from EUIPO on levels of counterfeited products within the clothing (the most pirated) sector. The estimates also support the general thread of the major brands’ arguments that the web has accelerated levels of and opportunities for counterfeiting, but until now there has been no way of calculating this. Given the paucity of offline data from government in relation to social media and the attendant reliance on anecdotal or ‘rule of thumb’ evidence, this data marks the first time we have become aware of the estimated levels of counterfeiting and piracy activity, not through forecast models but through tracked behaviour and surveyed attitudes.

6.0 Phase 3 Assessing the harm of purchasing counterfeit products using social media

6.1 Assessing harm and impact

This section relates to the impact of IPR infringement, as well as the characteristics of infringement, notably the consumer behaviour involved. There were a number of different methods considered to assess the impact of counterfeiting and the harm stemming from it, including the OECD's primary-versus-secondary market segmentation, which was adopted by BASCAP to describe non-obvious-versus-obvious copies, Hopkins et al.'s 'harm matrix' and various studies from GAO and, more recently, OHIM (now EUIPO)[92]. These were all helpful in identifying the different effects, including damage and harm (direct and indirect) to different stakeholders.

Stakeholders

When addressing the issue of the economic impact of counterfeiting activity, there were four basic parties to be considered:

a) *Industry/manufacturers.* These are the different sectors involved, including luxury brands, fashion goods, and alcohol and tobacco (both of which are impacted by high UK duties).

b) *Consumers.* These are our complicit, compliant, deceived and unexposed consumers of the products.

c) *The social media sector.* These are all those firms involved in the online world. This sector mainly covers Facebook and Twitter, but also includes online marketplaces like eBay/Amazon and search engines like Google and Bing.

d) *Government.* This is affected in terms of both its tax revenues and consumer interests.

92 Other sources are identified in the literature reviews summarised in the various stages of Phase 1 of the research outcomes. Appendix 5 also provides an assessment of behavioural economic approaches and two mathematical models, one on the economic impact on industry and the other on the drivers of complicit behaviour.

Harm

Through the examination of the literature the following key elements should be used to assess the harm from counterfeiting:

a) Brand reputation. This is the extent to which, where the degree of deception is high, counterfeiting can cause harm to the manufacturer of the authentic product. According to our interviews with industry, this was a key concern, particularly as deception online was much easier to achieve than deception offline. It also featured as a concern in the private enforcement agencies' reports.

b) Primary versus secondary/non-obvious versus obvious. This illustrates the different impacts on consumers and is crucial to distinguishing the different types of consumer behaviour involved. Here, the damage or harm relates directly to the consumer. According to the consumer tracker and survey, the number of consumers who were deceived was far lower than the number of consumers who were complicit, but MarkMonitor and others have suggested that the proportion of those who were deceived in online purchases is growing.

c) The harm matrix. Hopkins et al.'s typology of harm expands on the above primary-versus-secondary market distinction and categorises ranges of harm as follows: high quality/high deception, high quality/low deception, low quality/high deception and, finally, low quality/low deception.

For our purposes, we must assume that the greatest harm and damage to both consumers and brands is concentrated in low-quality/high-deception goods, with the consumer left feeling cheated and the brand, according to industry sources, being blamed. There is also the potential harm to the consumer with goods such as fake hairdryers, where there are clear health and safety issues. This typically occurs when the goods are sold in near-perfect packaging while the goods themselves are inferior and unsatisfactory, thus representing the greatest level of deception.

We believe that high-quality/high-deception goods would have the greatest financial impact on brands, as these would most likely represent lost sales to the brand. High quality/low deception may be of most benefit to consumers and is most likely to appeal to complicit consumers; these are arguably (at least according to some) not lost sales for the brands, as these consumers would not have purchased the authentic goods at the authentic price in the first place.

What is clear is that high levels of deception, rather than high levels of quality, are the cause of the greatest harm, with high-quality deceptive purchases being harmful to industry, and low-quality deceptive purchases being harmful to both industry and the consumer.

d) Price. Morales[93] notes the impact of price, as well as quality differences when purchasing counterfeits, with consumers more likely to buy counterfeit products when the price of the original is significantly higher than that of the counterfeit and when the

93 Morales, A.C. (2005). 'Giving firms an "E" for effort: consumer responses to high-effort firms'. *Journal of Consumer Research*, 2005, 31, pages 806–12.

quality of the counterfeit is sufficient. He also suggests that the consumer's feelings about the company making the original product are important.

This means that, as the difference in price between the original and the counterfeit product increases, this will increase consumers' readiness to buy the counterfeit. By contrast, as the difference in quality between the original and the counterfeit product decreases, this will also increase the likelihood of consumers buying the counterfeit. Morales also claims that the difference in quality moderates the effect of the difference in price on the consumer's purchase intentions. In our view, the price consideration may apply mainly to complicit consumers, but in e-commerce, where consumers are looking for if not expecting an online discount, there is clearly scope for them to be deceived by clever pricing.

In terms of relating this to social media, it could be argued that low-quality/high-deception goods are the ones industry and enforcement agencies have claimed are likely to be sold on platforms with near-identical, if not cloned, images from authentic goods websites; these are used to deceive the consumer into purchasing them. These may just as easily be offered in open groups, which could add to the sense of authenticity. This may also be true of high-quality/high-deception goods, where the pricing may be closer to the authentic price to attract a purchaser looking for an online discount. This is typical of certain products where the reproduction of the goods is near perfect, such as DVD box sets. Equally, the kinds of goods often being disseminated across closed groups seem to be high-quality/low-price products, where damage may be limited. The direct and indirect impact on the main three stakeholders – industry, government and consumers – from social media can be assessed as follows:

- *Direct impact.* Industry has been seeing a loss of revenue because of the potential substitutional impact of counterfeits on authentic goods, particularly where there is a high degree of deception, although this is lower if the goods are non-deceptive. This represented the most likely impact of social media where the platforms enable the dissemination of deceptive counterfeit goods.

- *Indirect impact.* For industry, this is the result of reputational harm from the low-quality/high-price goods that are common on social media (according to industry and enforcement agencies).

- *Indirect impact. T*his is the impact on government due to the loss of employee and corporate taxes and the impact on employment. There is a widespread belief that much of the activity emanates from and profits are made by counterfeiters in China and other Southeast Asian markets. There is also the cost to government of having to enforce IP infringements, such as the activities of Trading Standards.

Indirect impact. For consumers, there may well be a welfare benefit (recognised by GAO) for certain types of products (high quality/low price), but for almost all other types of products however the impact is direct.

6.2 Overview

According to our tracker and survey data, social media affected the sales volume of counterfeit goods, and there could be little doubt that social media was having a substantial social impact and changing the way consumers interacted with suppliers. That there is evidence that social media increases the likelihood of the acquisition of counterfeit goods should not be surprising.

Restricting the supply of 'grey goods', combined with ensuring that consumers can make an informed choice, are two key steps towards limiting the negative impacts of counterfeit goods. This should form part of any education and awareness campaign and illustrates the need to inform consumers more effectively. It also supports our conclusion that more resources are needed on the demand side of this issue to understand consumers' motives and attitudes more easily.

We also aimed to provide insight on other research objectives, including the impact of social media on producers' reputations (see Appendix 5). However, this was not clearly demonstrable from the research despite claims made by industry (notably private enforcement agencies) about the damage caused by fake websites, including social media pages, on brands' reputations. In relation to opportunities for countering infringement, we felt that this requires a great deal more work, not least in improving education and awareness, as well as in terms of social media platforms investing in efforts to actively counter IP infringement. The avowed zero-tolerance attitude of Google to trademark infringement and the anti-fake drugs campaign by Microsoft's Bing platform have shown what can be done to help industry and government counter infringement. Trading Standards provided a unique perspective on why particular social media channels are used over others (essentially, it was a matter of cost), and the consumer survey data highlighted how and why particular sectors of goods were targeted.

7.0 Summary, Recommendations and Conclusions

7.1 Research outcomes summary

Scale of infringement

Even though search engine Bing showed that there is a role for educating consumers about the dangers of counterfeit goods, there was little evidence that social media has been used to promote IPR. By contrast, there were many claims, from both industry and government agencies, about its role in facilitating IPR infringement, sometimes flagrantly. How infringement was distributed between the different sectors, products and types of IP was not always clear, but the survey and tracker indicated that certain goods (like tobacco and alcohol) were less likely to be promoted on social media. However, views expressed in the industry survey and road shows indicated that almost every ACG sector was impacted, just to varying degrees. The paucity of current scaleable official data, combined with the lack of current industry data and unverifiable industry claims, made it difficult to reliably assess the scale of infringement. This means we had to rely on data from the consumer survey and tracker to reveal how social media can contribute to facilitating infringement. We note the high levels of suspect transactions revealed by the tracker, but this data needs to be supported by further regular frequent tracking of online consumer behaviour. Nonetheless, the scale of infringing activity indicated by the consumer data bears out many industry claims.

Impact of infringement

We explicitly included this issue within our questionnaire and the responses indicated that the impact varied across the different sectors, with some firms blaming the rise of social media for an increase in levels of counterfeiting and thus damage to their business. None of the firms surveyed were able to specify the actual costs to their business, and we attributed this to industry's historical reluctance to share confidential financial information and a recognition that major brands readily engage with social media for sound commercial reasons, albeit sometimes as a defensive measure. It was clear that the social media platforms use similar 'safe harbour' defences to resist attempts by industry to get them to adopt more proactive policies for combating infringement. This reactive attitude has created a climate of distrust and suspicion between these platforms and rights holders, which is made worse by what are seen as cumbersome takedown policies. The social media platforms argued that the IPR system within the UK is very fragmented and is part of an even more complex system across 150 other countries. While consumers who use social media are able to enjoy many positives, the dark side of internet-based commerce is shown by the ease with which both websites and social media pages can be manipulated to deceive consumers (although, from our findings, we still regard such deceived consumers as a small minority of those who use the platforms). The main focus for blatant infringement, according to industry and government agencies, is

the proliferation of closed groups (i.e. invite-only groups, created on social media platforms). These groups clearly have a strong influence on infringement and this belief is borne out by our consumer research data, which indicates that IPR infringement is five times more likely in closed groups than in open groups. We consider this the most important finding of the project.

Characteristics of infringement

There were claims from industry and government agencies about the flagrancy with which IP-infringing content is placed on social media, although only FACT provided us with meaningful examples. We relied on explanations from the private enforcement agencies as to how counterfeiters were able to copy near-identical images from legitimate sites to deceive consumers. In certain cases, this involved near-perfect copies of certain products being priced close to the authentic article, completely bypassing the legitimate brand owners' distribution and retail system. This infringing activity took place across myriad online platforms, not just on social media. The consumer data provided by us pointed to these deceptive copies as a growing threat, albeit one that still represented a small part of total infringing behaviour on social media. Deceptive purchases were more likely to occur with products like clothing, but were not characteristic of every impacted sector and product, least of all alcohol and tobacco. The bulk of infringing activity tracked in this study involved complicit consumers. However, we are aware that the use of VPN and the dark net[94] means that much of the current online illicit activity is beyond oversight and reach. On social media platforms, the increased use of spambots and links to various payment sources off-site makes it harder than ever to control the full scope of illicit activity.

Opportunities for IP

Microsoft's Bing search engine has shown that online technology platforms can take an active role in combating IP infringement; in their case, this related to the offering of counterfeited drugs online. Google's statement in relation to trademark infringement was compelling given its avowed zero tolerance for counterfeits, and we note the improved cooperation between eBay and rights holders. Recent changes to Facebook's business model suggest that there may yet be opportunities to improve IP awareness, especially as they become more reliant on advertising from the brands whose goods are infringed within their platforms. It was evident that the online platforms are most likely to act against illicit activity on their sites if their own business interests are under threat. Education and awareness campaigns to date have illustrated the need to better inform consumers, but in relation to opportunities for countering infringement this area still required much more work and greater investment by the social media platforms in efforts to actively counter IP infringement. In the absence of greater cooperation from industry in supplying data, the focus of future research should be placed on disrupting the current levels of consumer complicity and this is one area where the social media platforms could have a role to play.

94 VPN is a virtual private network which uses a public network such as the internet to connect to a private network such as a company's intranet. The dark net is an overlay network that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports - Wikepedia.

7.2. Conclusion and recommendations

Efforts to benchmark and compare data from the three key sources (government, industry and consumer) have only been partially successful. The methodological problems that beset most official data and estimates, as well as industry's reluctance to share confidential and often real-time information, render these first two data sources as inadequate measures of illicit activity in this market. None of the three main private enforcement agencies contacted were willing to supply us with more than headline data, even in anonymised form, that would have provided current insights on the scale of illicit activity on social media and other web platforms. This meant we had to rely on unverifiable assertions and claims made by these firms at conferences and within their published reports. That said, these 'private' enforcement agencies were better informed about current online (including social media) infringements of IPR and seemed best placed to provide current updates on their work. We recommend increased industry cooperation in supplying essential headline data for government and policy makers to understand more easily the trend in the market. This privileged and confidential information is always a more current and accurate reflection of the market than the data available from government and official sources, which are either out of date or methodologically unsound. Nonetheless, our tracker and consumer survey data provide meaningful, current (albeit snapshot) data, notably on segments such as levels of deception in online purchases and the 'generation' gap in online consumer attitudes and behaviours. There is also a strong argument for making more out of existing as well as new data sources and the technologies for capturing digital activities. This is a point made by Coyle [95] in citing a key finding of the interim report of Sir Charles Bean's Review of Economic Statistics.[96], [97]

Conclusive findings from our consumer data are somewhat restricted as the online tracker only captures complicit behaviour. Capturing deceived behaviour would require an augmented approach, starting with mystery shopping, to identify the relevant links and then track them. However the data shows that;

a. Online groups are self-organising, involving herding. This is comparable, from an enforcement viewpoint, to activities within terrorist cells.

b. Despite the emphasis placed on the threats posed by closed groups, opportunities exist in open groups to secure new users and these represent the greatest threat from social media in amplifying the counterfeiters' messages. Even if the open groups are shut down, they can easily be set up again.

c. Social media amplifies the counterfeiters' messages by increasing the connectivity of potential complicit consumers. Crucially, these connections do not have to be strong; as can be seen from network effect sources, the threshold for connection on social media is low.

95 Coyle, D. (2016) 'The Sharing Economy in the UK' [Online]: http://www.sharingeconomyuk.com/perch/resources/210116thesharingeconomyintheuktpdc.docx1111.docx-2.pdf
96 UK Government (2016) 'Press notice: "Take economic statistics back to the future," says Charlie Bean' [Online]: https://www.gov.uk/government/publications/independent-review-of-uk-economic-statistics-final-report/press-notice-take-economic-statistics-back-to-the-future-says-charlie-bean
97 Bean, C. (2016) Independent Review of UK Economic Statistics [Online]https://www.gov.uk/government/publications/independent-review-of-uk-economic-statistics-final-report

More reliable and meaningful insights can be gained from consumer data such as ours and there should, in the future, be a much greater focus on researching the demand rather than the supply side of counterfeiting. The consumer data presented in this study have shown how social media plays a role in facilitating IPR infringement, particularly in closed groups, but the data presented represent a mere snapshot from the middle of 2015. The lack of any other comparable data means these cannot be used to provide a definitive indication of the development of this phenomenon over time. A methodology that allows an assessment of both stated and revealed preferences, such as the one we have employed within this study, is, we believe, desirable as a more effective and reliable measure of illicit activity.

We also believe that there is a need for a single methodology for more frequent, longer-term research (comparable with the Ofcom/Kantar survey for online copyright infringement) to provide a unique data set as the basis of an official national measurement. We would argue that developing a greater understanding of consumer motivation for purchasing counterfeit goods is pivotal at this time.

Our findings suggest that consumer behaviour is nuanced and encompasses complicit behaviour (favouring non-obvious copied goods), which has a lower economic impact, and deceived behaviour. It tends to involve high-quality/high-priced goods and represents a greater potential threat to brands in the future (even though, at present, these deceived consumers make up a small proportion of the total consumers impacted by counterfeit goods, online and through social media).

The full extent of the challenge from social media may not be entirely clear from this study, but from industry sources we believe that it is growing and will include more deceived consumers as the sophisticated tactics from the counterfeiters become ever more elaborate. We considered other challenges that may yet exceed those posed by social media, and these include: the arrival of messaging platforms suitable for mobile use, where it is harder to track illicit behaviour, given their embedded encryption technology; blockchain technology, which may enable counterfeiters to further hide the financial benefits of their activities; and 3D printing, where the potential exists to considerably increase infringement across all the main IPR. Most of this activity could occur outside any kind of scrutiny.

8.0 Appendices

Contents

Appendix 1: Industry Survey Responses

This contains the verbatim responses from FACT and various ACG members (in anonymised form) to our questionnaire.

Appendix 2: Enforcement Agency Survey Responses

This represents the verbatim responses from the IPO Intelligence Hub and Trading Standards' eCrime unit to our questionnaire. The Trading Standards response is prefaced by a summary of a telephone interview.

Appendix 3: Technology Firms' Survey Responses

This includes a summary of our interactions along with the verbatim responses from the three technology firms we approached. Rather than respond to our questionnaire, each firm supplied its own set of terms and policies used in relation to trademark and (in the case of Twitter) copyright infringements.

Appendix 4: Consumer Tracker and Consumer Survey Results and Analysis

This includes:

Appendix 4.1: Key definitions used

Appendix 4.2: Gini curves of the distribution of exposure for the different search engines

Appendix 4.3: Consumer survey methodology

Appendix 4.4: Behavioural analysis from social media

Appendix 5: Economic Models and Approaches

This includes an assessment of behavioural economic approaches and two mathematical models, one on the economic impact on industry and the other on the drivers of complicit behaviour.

8.1 Appendix 1: Industry Survey Responses

8.1.1 FACT survey response

Q1. How do you enforce your intellectual property rights (IPR) online and offline?

Online

FACT uses a wide variety of methods to deal with copyright-infringing websites. Some of these methods are:

I. Closing the website via:

   a. Domain sign overs

   b. Liaison with hosting providers

   c. Liaison with domain name registries

II. Detection:

   a. Scanning systems to detect member content online

III. Removing infringing content:

   a. Takedown notices (DMCA notices)

   b. Auction website removal tools (e.g. eBay's VeRO program)

IV. Reducing website popularity:

   a. Website blockings

   b. Search engine delisting

   c. Social media page removals (Facebook and Twitter)

V. Restrict website revenue:

   a. Remove payment providers (e.g. Visa, PayPal, etc.)

   b. Remove advertising (via liaison with brands/ad networks)

Offline

FACT targets those who seek to acquire content at UK cinemas by recording films. The increasing use of the Intelligence Unit and Internet Investigation Team, alongside the Theatrical Investigator, has led to a multifaceted approach to tackle this. FACT now identifies and develops intelligence in-house, which culminates in operations to successfully arrest or deter web-cammers. The Theatrical Investigator has a preventative mandate, educating cinema employees through training programmes and rewarding them via incentives. This work is funded by the Film Distributors' Association (FDA), which is the trade body for theatrical film distributors in the UK.

FACT assists the UK Border Agency with a variety of customs seizures. Large seizures of High Quality Pressed Discs (HQPDs) of all the latest television and film boxsets are frequently intercepted on their way into the UK. Invariably, these shipments have originated from China or Hong Kong. FACT frequently examines a small sample of each seizure to confirm that the product is counterfeit.

Large-scale shipments of Internet Protocol Television (IPTV) boxes are also frequently intercepted. These devices are usually illegally preconfigured with software that enables them to unlawfully access television, film and live sports content via the internet, free of charge.

Customs intelligence is collated by FACT to identify the large-scale suppliers in the UK and the common overseas sources of the counterfeit product. Often, links between large shipments and online suppliers can be found, which assist with the progression of FACT's cases.

Q2. Are your strategies for online and offline commerce interlinked, e.g. do you treat the internet as a shop window for physical goods?

Yes. FACT's role in successfully detecting and targeting those involved in such crimes requires the ability to foresee and react to developments in technology. Criminals are often the pioneers of these developments and are quick to take advantage of the ever-changing landscape to create methods to profit from delivering stolen content to a wider global audience.

FACT's work in protecting its members' intellectual property now focuses predominantly on illegally acquired content, accessed via websites that offer direct downloads, file sharing or streaming.

Even the dwindling hard goods market has been altered by technological advancements. Social networking websites are now an integral part of modern life. Currently, there are over 1.49 billion active users on Facebook and it is increasingly being used as an online platform for DVD sales. This is in addition to direct sale websites, online marketplaces and auction websites like eBay. These methods are replacing the 'traditional' hard goods sales methods (i.e. street sellers, markets and car boot sales).

Q3. How do you collect data on infringement of your IPR for your internal purposes and, where appropriate, for presentation to policy makers (if there is a difference)?

a. Public complaint reporting system (via online form and phone calls)

b. Partnership with Crimestoppers

c. Information-sharing agreements with LEAs in the UK and overseas

d. FACT is a member of the National Anti-Fraud Network (NAFN)

e. FACT works with the Intellectual Property Office

f. FACT members

g. Industry contacts

h. Scanning systems to detect member content online

Q4. As regards the seasonality in the levels of IPR infringement, if there is any, what are your observations?

There are only three main periods in the year when FACT witnesses any seasonality in IPR infringement:

i. **August/September** – High levels of intelligence at the start of the football season every year as new illegal live-streaming websites emerge online. In addition to this, FACT witnesses an increase in complaints, at this time of the year, regarding public houses that are showing live sports to their customers via an illegitimate means (domestic subscription, foreign satellite service, IPTV device or control word-sharing network).

ii. **December** – High level of complaints regarding the sale of counterfeit DVDs online leading up to Christmas.

iii. **December/January** –There is high release group activity leading up to the movie awards season (the Oscars and BAFTAs are both held in February). The film industry sends out advance copies of recent movies to critics and awards voters. Often in DVD format (but now also in Blu-ray), these high-quality releases are much sought after online and as a result are subjected to intense security by the studios sending them out. Despite all the precautions, leaks can happen. Every year copies of DVD screeners (identified by the term DVDSCR) turn up on torrent sites and are downloaded in huge numbers.

Q5. Please describe the scale and impact of infringement of your IPR on your established goods, your newly launched goods and your brand in general.

IPR infringement has a huge impact on all FACT members' content. Television and film content will only be produced if studios can make a return on their investment. The average Hollywood movie costs $60–100 million to produce. The revenue generated back from movie sales will not only cover the cost of making the film but also the cost of investing in future projects. Studios look to gain a return on their investment via the box office, the subsequent DVD, Blu-ray and download sales and the distribution of the broadcast rights to television and online streaming services (e.g. Sky Movies and Netflix). All these areas are threatened by IPR infringement.

Sports broadcasters are affected in a similar fashion. Earlier this year, Sky and BT Sport (FACT members) agreed to pay a record £5.14 billion for the live Premier League TV rights over three seasons from 2016–17. This represents a 70% increase on Sky and BT's current £3 billion deal. This is just one of several leagues/sports that these members have invested in for the viewing pleasure of their customers. This is only financially viable if they make a return via their domestic and commercial subscriptions. Therefore, individuals who offer these broadcasts illegitimately for their own financial gain threaten this investment.

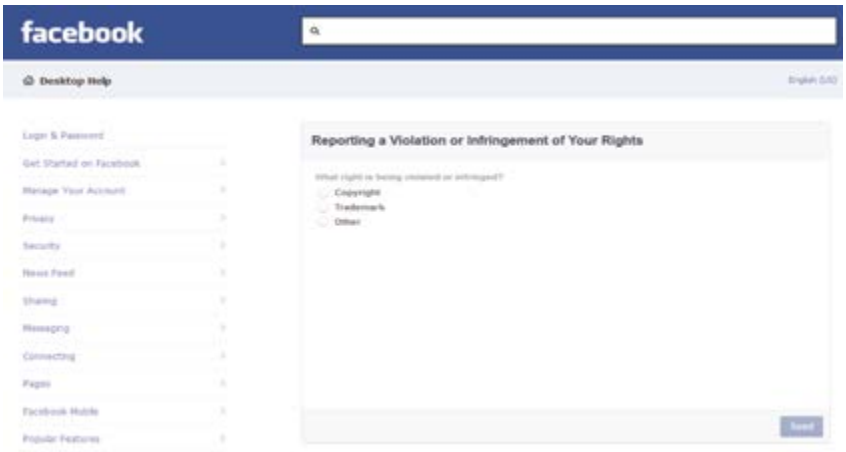
Q6. What procedure do you apply towards IPR infringement on the platforms of online services, e.g. do you contact them directly and if so, how? Is there a specific procedure in place for social media platforms?

FACT has procedures in place to deal with copyright infringement on the following websites:

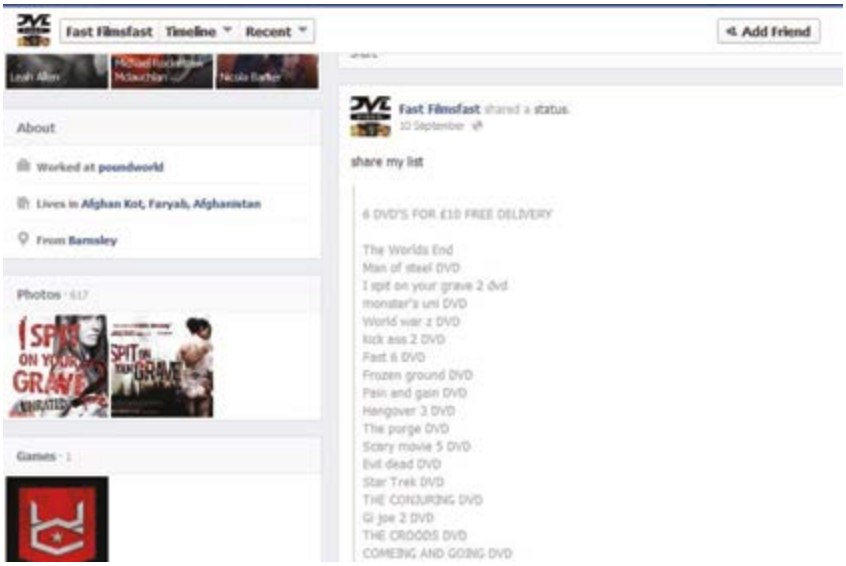
i. **eBay** – FACT is part of eBay's VeRO Programme to remove any infringing auction listings via an online form.

ii. **Twitter** – FACT frequently uses Twitter's online copyright infringement reporting tool to remove tweets and Twitter accounts.

iii. **Facebook** – Facebook provides an online reporting facility (shown below) for rights holders and members of the public to report violations that include copyright and trademark issues. In December 2012, FACT incorporated this procedure into its 'alternative to prosecution' strategy. FACT has had some success in using this reporting tool. Often, Facebook will remove specific posts rather than the whole profile or community page. On occasion they will remove entire groups if repeat infringement is shown.

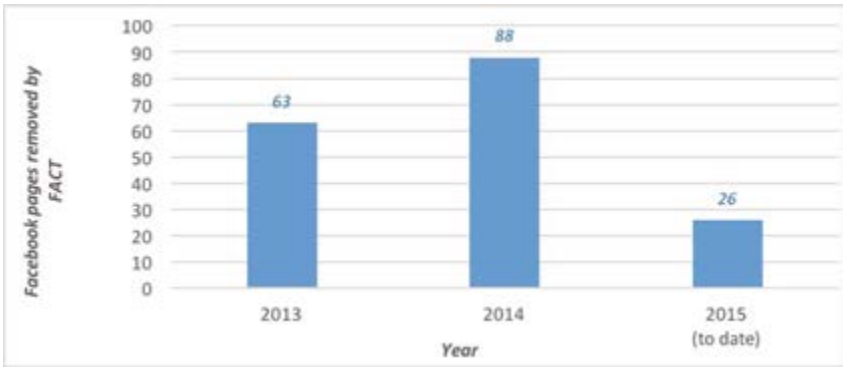


Reporting tool case study – On 17 September 2013, FACT reported a page called Fast Filmsfast (www.facebook.com/knockoff.nigel.790) via the Facebook reporting tool.The page was illegitimately selling the latest DVDs for sale (see below).



On the same day, Facebook disabled the account and the following notification was displayed:

Since 2013, FACT has used the Facebook reporting facility to remove 177 Facebook pages on the grounds of copyright infringement (see bar chart below).



The figure for 2015 may seem relatively low, but it was expected to rise significantly by the end of the year, as the months leading up to Christmas usually involve high levels of intelligence regarding infringing activity on Facebook. In addition to this, FACT was due to participate in a multi-agency initiative over a two-week period in November 2015, which aimed to address IP crime on Facebook.

Q7. In your experience, how significant are social media platforms in facilitating online infringement of your IPR?

Social media has an influence on almost every type of copyright infringement that FACT investigates:

i. **Source piracy** (film/TV) – Release group, Facebook profiles/fan pages and Twitter accounts

ii. **Copyright-infringing websites** (film/TV/live sports) – Facebook profiles/fan pages and Twitter accounts with the latest available torrents, streams, downloads and website news

iii. **Copyright-infringing apps** (film/TV/live sports)

iv. **Hard goods DVD sales** (film/TV) – Facebook profiles advertising all the latest film and television content for sale on DVD

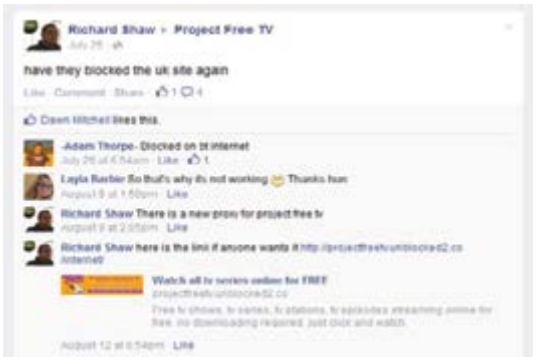
v. **Premium TV broadcast interception** (live sports/TV) – Facebook profiles advertising card-sharing services and IPTV boxes for sale

Source piracy

Release groups are organised groups of individuals dedicated to providing pirated versions of the latest content, such as films or television episodes. Release groups will frequently have an associated Facebook account where multiple hyperlinks advertise the online locations of their latest copyright-infringing content. An example of this is shown below in a screenshot, which displays a Facebook page for Heaven Killers Release Group. The screenshot shows that this page has accumulated 18,150 likes. On the right is a post from the group advertising seven websites where their illegal release of the Paramount Pictures film title Noah was available.

Copyright-infringing websites

Social networking sites are used in a variety of ways by copyright-infringing websites, their owners, admins and users alike.



A large number of 'pirate' websites will have an associated Facebook or Twitter account, with Google Plus and YouTube accounts also seen on a regular basis. These are very often open groups, as they want to attract as many online users as possible.

Social networking accounts are often used to promote and advertise these websites and are usually linked to the website itself.

They are often used to promote new content that has been added to a website, and they regularly link directly to downloadable files, torrent files or pages on their website where content can be viewed.

From experience, if a link on Facebook/Twitter takes users directly to copyright-infringing content, the social networks will, upon receiving a DMCA notification, remove the specific posts. On occasion they will remove entire groups if repeat infringement is shown.

For example, the screenshot below shows a Facebook page for *YIFY Torrents*. The website *yify-torrents.com* is a popular torrent site which provides access to TV and film content via torrent files. This Facebook page has accrued 198,134 'likes' from users and it can be seen that it displays the URL for the torrent website as well as regular links to newly available content. The Sony Pictures film title Paul Blart: Mall Cop 2 is shown in the second screenshot below (this movie was still airing in cinemas at the time and hadn't yet been released on DVD or Blu-ray).

In light of the UK website blocking orders in recent years, it has also been observed that users of 'pirate' websites are making use of the Facebook platform to discuss ways around the block, making suggestions for circumvention.

For example, the popular illegal website Projectfree.tv was blocked by ISPs in the UK in November 2013. The top right image shows users of the Project Free TV Facebook page openly discussing the blocking of the site by BT. Another user, in response, provides a link to a proxy for the website that allows UK users to freely access the site.

Four days later, users then started to discuss that Sky had also now blocked access to Projectfree.tv and a user is requesting ways to circumvent the block. "Any suggestions to get around the block?" (Right).

As shown, another user soon after makes a suggestion for a free proxy and a VPN service, both of which would allow the UK users to access the blocked site and view copyright-infringing content.

Twitter is also used in a similar manner, as users tweet and share links to content that is newly available on copyright-infringing websites. For example, a popular copyright-infringing website, Flixanity.com, was brought to FACT's attention in 2014. The site had an associated Facebook page and a Twitter account, which were used to provide followers with direct links to movie and TV content as it became available on the website, in just a single click. The Twitter page is displayed below:

Copyright-infringing apps

Using Facebook to distribute copyright-infringing apps is also now a popular use of the social network. For example, the app ShowBox is not available on any of the legitimate app stores like Google Play or Apple but the APK file (Android application package) can be downloaded directly from the link published on its associated Facebook group page. This app will run on any Android device.

The screenshot below shows a link that has been posted on the Facebook page for the APK file to be downloaded directly.

Social networking sites are also used to advertise sports streaming websites and regularly provide a way to share direct live streams that can be accessed by users in a variety of ways. The first example below advertises a private sports streaming website, offsidestreams.com, which requires a paid subscription in order to view the content. As shown in the displayed post, the group is directing potential new customers to a secondary domain to gain new registrations and ultimately additional revenue for paid subscriptions.

The second example, below, shows a Facebook group that posts links to watch the Sky Sports 1 and Sky Sports 2 channels online without a legitimate subscription to Sky services.

Hard goods DVD sales

In recent years, we have observed a decline in counterfeit DVDs being sold in person (by street sellers or at markets and car boot sales). Conversely, during this time we have seen a surge in the number of Facebook pages dedicated to selling the latest films and television series on DVD. Facebook provides a certain amount of anonymity for these individuals, which makes any kind of law-enforcement activity particularly difficult to address. The screenshot below shows a Facebook page for Mike's Movies (www.facebook.com/mikesmovies4u), a profile set up solely for the purpose of advertising and selling counterfeit DVDs at £2 each or six for £10. Although Facebook does not process payments, clearly this page has been set up as a store. Orders and payments are usually dealt with via private message. A clear benefit to the operator of this page is the visible endorsements from its customers (pictured below) regarding the quality of the counterfeit products on offer.

Premium TV broadcast interception

The illegal broadcast of premium television content, including live sports events such as Premier League football games, predominantly occurs via three different methods:

1. streaming and indexing websites (discussed earlier)

2. TV control word-sharing (CWS) networks – also known as card-sharing networks

3. illegally preconfigured IPTV boxes.

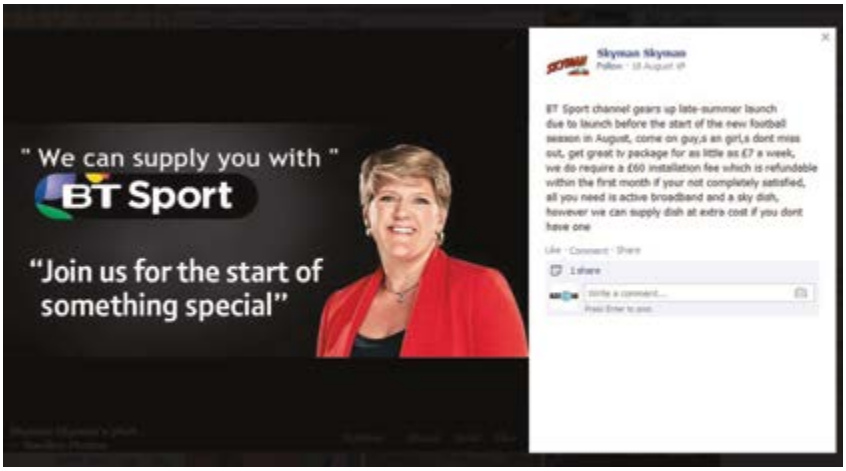
Facebook is frequently used to advertise the sale of infringing broadcast access through illicit set-top boxes (STBs) and IPTV devices. The STBs that are set up on a CWS network are usually offered on a subscription service, whereas the preconfigured IPTV boxes can be sold for a one-off payment. These services are sold to both domestic and commercial customers.

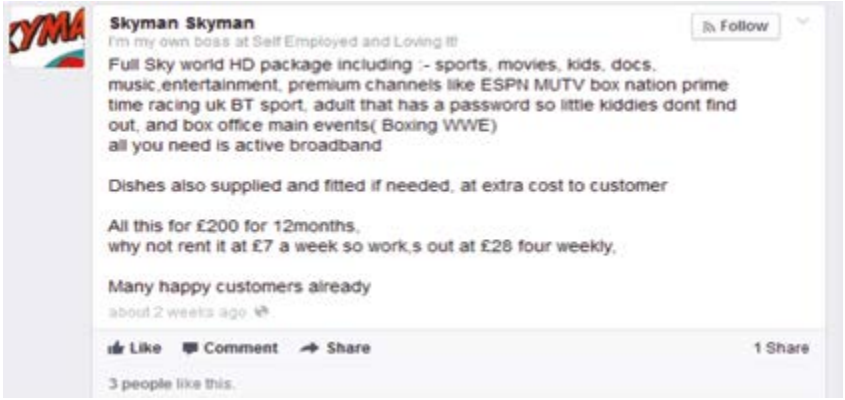
An example of the use of Facebook is shown in the screenshots (right), whereby the user Mark Xbmc Kodi Schofield was identified as selling IPTV boxes for £80, providing users with illegitimate access to Sky television services.

The sale of these so-called 'free' Sky services can be extremely lucrative. As shown in the supplier's Facebook message, he received 446 messages in three hours relating to the illicit service he was advertising.

The user for this service provides customer service via Facebook, interacting with his customer base to resolve issues, as well as organising times to visit his clients directly (below). Facebook has been found to be both a promotional tool as well as providing on-going customer support. Users of the systems will frequently comment on the systems and provide reviews of the services.

A second example can be seen below whereby the Facebook profile Skyman Skyman is advertising illegal satellite access to BT Sport packages for £7 per week, with an installation fee of £60.

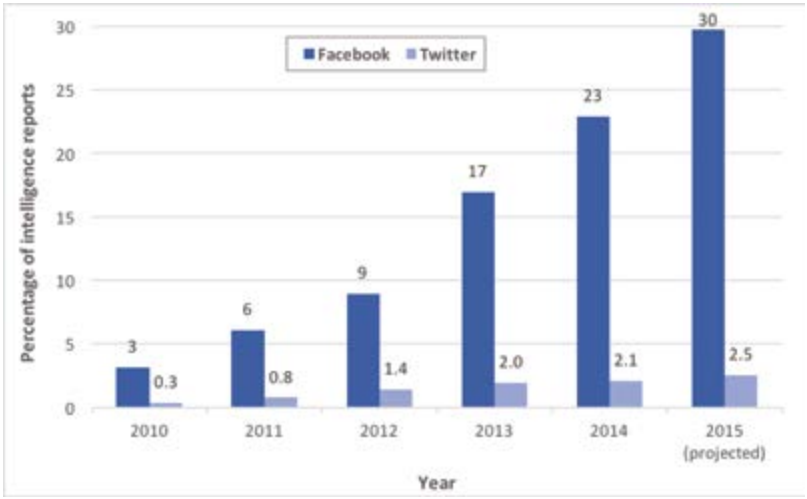




Q8. What, in your experience, are the scale and the characteristics of infringement of your IPR on social media?

Social media plays a crucial role in assisting intellectual property infringement in the vast majority of FACT's investigations. The use of social media by individuals and groups infringing FACT members' content is continually rising. Social media is usually adopted to enhance existing illegal services (hosted on third-party infringing websites) by keeping users updated with new content and news. However, in some instances, as with DVD sales, social media can provide the platform for the entire illegal operation.

Over the past five years, we have observed a significant increase in FACT intelligence reports on copyright infringement that also mention specific social media profiles (see graph below).



Q9. Have you seen a rise in the infringement of your IPR over the past five years and to what do you attribute this, e.g. improved delivery mechanisms or new 'platforms'?

It is incredibly hard to quantify the level of infringement at any given time, so unfortunately we cannot accurately comment on any potential fluctuations.

Q10. In your experience, are social media platforms used to offer physical goods infringing your IPR? If so, please list them.

Please see answer to question 8.

Q11. What, if any, economic impact do you consider social media to have on your IPR, both in terms of infringement and enforcement of your IPR?

IPR infringement negatively impacts the creative industries, which currently employ 1.8 million people across the UK.[98] The value of the services exported by the creative industries in 2013 was £17.9 billion. In total, exports of services from the creative industries accounted for 8.7% of total exports of services for the UK in 2013.[99]

98 'Creative Industries: Focus on Employment (2015) by the Department for Culture Media & Sport'.
99 'Creative Industries: Focus on Exports (2015) by the Department for Culture Media & Sport'.

Social networking websites are now an integral part of modern life. Globally, there are currently over 1.49 billion active users on Facebook and 316 million active Twitter accounts. This provides the perfect opportunity for criminals to:

- direct the public to infringing content hosted on other websites
- advertise and sell infringing products
- provide on-going customer support for their illegitimate services

Conversely, social media websites such as Facebook and Twitter are rich in open-source data, which FACT has repeatedly found to be invaluable intelligence sources during online investigations.

Q12. What problems do you encounter in practice when trying to enforce your IP rights?

Fake/hidden website registration details – Website registration details are often fake or hidden, which provides no further links to the person controlling the domain and its illegal activities.

Overseas servers – Investigating servers located offshore cause some specific problems for FACT's law-enforcement partners. In order to complete a full investigation into an offshore server, a law-enforcement agency must liaise with its counterpart in the country where the server is located. The difficulties of obtaining evidence from other countries are well known.

Torrent websites and DMCA compliance – Some torrent website operators who maintain a high DMCA compliance rate will often use this to try to appease the law, while continuing to provide infringing links.

Current legislation too vague to remove infringing live sports streams – Current legislation is insufficient to effectively tackle the issue of websites illegally offering coverage of live sports events. Section 512 (c) of the Digital Millennium Copyright Act (DMCA) states that: upon notification of claimed infringement, the service provider should "respond expeditiously" to remove or disable access to the copyright-infringing material. Most live sports events are under two hours long, so such non-specific timeframes for required action are inadequate. The law needs to reflect this narrow timeframe with a specified required response period for websites offering such live feeds.

Camming content directly from cinema screen to the cloud – Recent advancements in technology have made this a viable option to 'cammers' to avoid detection. Attempts to curtail and delete illicitly recorded film footage may become increasingly difficult with the emergence of streaming apps that automatically upload recorded video to cloud services. While enforcing officers may delete the footage held on the device, the footage has potentially already been stored remotely on a cloud system.

Domain hopping and proxy websites – ISP-implemented website blockings are becoming increasingly commonplace in the UK. The targeted websites have begun to circumvent the blocking process by using proxy websites and moving to alternative domains outside those indicated in the court orders. Web browsers that use Tor to circumvent the UK blockings are also now freely available to download.

Virtual currencies – There is great potential in virtual currencies for money launderers and illicit traders. Government and law enforcement have raised concerns on how virtual currencies can be sent anonymously, leaving little or no trail for regulators or law-enforcement agencies.

Usability and appeal of the latest infringing streaming websites – New copyright-infringing BitTorrent websites are attempting to alter their image with slicker, more professional, user-friendly website designs. Websites such as Popcorn Time mimic the design and ease-of-use provided by legitimate services such as Netflix. Consequently, more people will inadvertently use illegal streaming services in the belief that they are accessing content legally. The improved simplicity of these illegal streaming services is likely to prove a significant factor for many users engaging with the website regardless of the legality, especially for users who do not have the technical capabilities that many of the BitTorrent sites require to obtain similar content.

8.1.2 Anti-Counterfeiting Group (ACG) members' survey responses

At the suggestion of the ACG, we set up the questionnaire as an online survey and received up to six responses. We have anonymised these and show the verbatim responses under each question to highlight differences and similarities.

Q1. How do you enforce your intellectual property rights (IPR) online and offline?

a) We monitor marketplaces, domains and social media online. We then enforce against any sellers/sites that are selling counterfeit versions of our products or using our imagery (taken directly from our website). We use MarkMonitor to enforce through to these platforms. In terms of offline enforcement, we use an investigation team to conduct TPs, etc.

b) Online we use external agents to coordinate the removal of suspicious listings. Offline we use local agents to authorise the destruction of seized goods and prosecution of sellers, as well as investigating the supply chain.

c) For trademark violations, we use in-house warning letters and external attorneys. Domain name violations: through UDRP (Uniform Domain-Name Dispute-Resolution Policy). Social media: direct contact with site (Facebook, Twitter, etc.).

d) Using manual searches, and lodging complaints manually with social media companies. We also use partners to search and enforce. Have own network of private investigators (PIs) and law firms across the world that assist with enforcement.

e) In the majority of cases we conduct enforcement through online monitoring.

f) We use a mix of methods: in-house reporting outsourced through MarkMonitor and via BrandStrike. We use tools such as MarkMonitor and IP Curator, as well as eBay and Amazon reporting tools. We also use Facebook and other social media reporting tools. We do not find much offline but we generally use PIs to find these and enforce our seizures at ports.

g) How long is a bit of string? We use all options open to us to enforce online and offline.

Q2. Are your strategies for online and offline commerce interlinked, e.g. do you treat the Internet as a shop window for physical goods?

a) Yes – we actively monitor the internet to identify potential infringers.

b) Yes, the online sales of counterfeit goods occur in areas with higher levels of offline sales and therefore appear to be linked.

c) Yes, they are interlinked. We treat the internet as a window to our products and services

d) To some degree. Scale and procedure implemented following detection differ.

e) Yes we do.

f) Yes. The sale of fakes at cheap prices damages our brand and our price structure.

e) Strategies are linked.

Q3. How do you collect data on infringement of your IPR for your internal purposes?

a) We manually collect data from online listings and request information from marketplaces such as eBay for our records.

b) Through our external agents.

c) Various internet tools like MarkMonitor and HootSuite. All data is presented to related persons and policy makers on a quarterly basis.

d) Record: jurisdiction, the right that is infringed and what product is being infringed. This is presented to policy makers to form strategies on how resources can be best used to tackle threats.

e) Before engaging the services of an online monitoring company I used to collect and report data manually, then place it on spreadsheets and report takedown values, volumes, regions etc. including from lost opportunities.

f) We use MarkMonitor. There is not much point in sending stuff to policy makers; they have lost the momentum. This is a battle we take on ourselves. However, we do supply ACG with data for policy.

e) Yes. Some info is confidential.

Q4. As regards the seasonality in the levels of IPR infringement, if there is any, what are your observations?

a) We tend to see a rise in counterfeit activity around September every year and then it peaks just before Christmas.

b) December and January have seen the highest levels of seizures.

c) Basically the same level year-round.

d) N/A. appears to be constant.

e) There does not appear to be a trend in the size of volume counterfeit sales and the relationship with the seasons. Some of our parts are low-value stock items £14.99 etc. they sell for £7.00.

f) Q4 and Q1 are bad for us (we are a fitness company) but it is pretty bad all year.

g) As we are seen mainly as a winter brand most infringements happen between Sep–March.

Q5. Please describe the scale and impact of infringement of your IPR on your established goods, your newly launched goods and your brand in general.

a) Established goods – we tend to see more counterfeit activity surrounding old products. Newly launched goods – counterfeit activity involving new product launches is seen less often. Brand in general – we are very active in IPR enforcement and the scale of infringement is isolated to specific locations.

b) The level of infringement on established goods is reasonably low. The levels, while low, are consistent and it is costly for the brand to continue to pursue counterfeiters and deal with seizures.

c) Since a majority of infringement involves our consumables business, infringement usually commences two to six months after a new model's introduction and moves through stages of knockoff/counterfeit to compatible and remanufactured.

d) Established goods: medium threat. There are a few older products that are continually infringed and appear to be infringed repeatedly. New: low. Brand: low. Main trade is clothing. Little clothing is copied; mainly accessories.

e) The scale of fake goods on our current brand is high in relation to cables, and car charges; newly launched product is not too much of an issue as we have now engaged the services of an online monitoring company. The brand was damaged through Amazon and eBay with bad customer reviews relating to bad experiences with our brand (albeit with fake goods).

f) Established brands suffer – we take down hundreds of listings a day. New launches are less of an issue for the first month and then it is bad, especially when we have heavy ad campaigns for a launch. That drives factories to make fakes quicker. The brand is well known and people seek cheap products, but generally delude themselves because it is easier to believe that it is a cheap deal, not a fake.

g) Huge, huge and huge.

Q6. What procedure do you apply towards IPR infringement on the platforms of online services, e.g. do you contact them directly and if so, how? Is there a specific procedure in place for social media platforms?

a) There are some online platforms that we contact directly and hold strong relationships with; others we contact using MarkMonitor. For social media platforms we use the relevant enforcement forms for each site.

b) We use our external agents for all online infringement, e.g. test purchases and taking down listings.

c) For social media we sometimes contact the page owner directly and ask them to remove the infringing material or we usually contact the site owner like Facebook or Twitter (through their complaint form) to take action.

d) We contact them directly. Social media is dealt with through their prescribed forms that are available online. Bidding platforms are dealt with through email communications.

e) Until recently I used to deal with the platforms directly. eBay was better than Amazon to deal with.

f) We use multiple tools, including MarkMonitor and the websites' own takedown services. For social media we use the Facebook reporting tool, which is painful but effective. The issue with social media such as Facebook is that the main sales happen in closed groups, which cannot be scanned easily. I developed a tool to scan these groups but it is time-consuming and Facebook are not helpful or supportive against a backdrop of major criminality on their platform from sexual predators, terrorism and many other larger issues. Most of the platforms are out of their depth.

g) Yes, we contact them directly and have procedures in place.

Q7. What problems do you encounter in practice when trying to enforce your IP rights?

a) In general we find that the majority of the Chinese business-to-business sites can be difficult to communicate with. In terms of social media we have had difficulty locating infringing content in the first place because of the restrictions on Facebook searching.

b) Difficulty in investigating the supply chain and determining the source of the counterfeits.

c) I have a strong feeling that the site owner's legal departments are woefully ignorant of IPR law.

d) Resistance from social media platforms. Establishing supply chains. Communication with the wider public.

e) Unless test purchases are made we are reliant on the images the seller has used to list the fake goods.

f) Time-consuming is the main issue. The length of time to find, report and await takedown.

g) Online, then, criminals are light years ahead of law enforcement and the law in general, making it easier than ever to commit crime. Other barriers to enforcement are the high costs of maintaining and enforcing rights. Lack of cooperation from online platforms.

Q8. In your experience, how significant are social media platforms in facilitating online infringement of your IPR?

a) Social media platforms act as a shop window for counterfeit activity. Facebook in particular proves to be a favourite for counterfeit sellers. We often find infringing content coupled with other brands on Facebook.

b) They have a low impact.

c) It seems like anything goes with these social media platforms. I have discovered porno sites using our TM that had been active for months.

d) Increasingly significant. Forms around a fifth of all infringement.

e) Not too sure how to answer this question.

f) The social media platforms are awful. A cynic may say that it is deliberately awkward.

g) Five out of ten.

Q9. In your experience, are social media platforms used to offer physical goods infringing your IPR? If so, please list them.

a) Yes – Facebook is used to sell counterfeit products in local selling groups etc.

b) No.

c) Yes: Instagram, Facebook.

d) Do you mean sites like Facebook? In the main the damage in the UK is carried out using Amazon and eBay.

e) Yes, Facebook in particular is used. It has taken over from eBay and Gumtree as the major area of concern. Selling pages and closed groups are a problem. Instagram is a problem, but less so.

f) Yes, footwear, accessories, clothing.

Q10. What, if any, economic impact do you consider social media to have on your IPR, both in terms of infringement and enforcement of your IPR?

a) Hard to tell at this point.

b) There is a light impact on the economics of our business.

c) There was not a budget for this issue two years ago. We have had to invest a significant amount of $$ into combating this issue at a company global level.

d) Hard to quantify as the level of scanning we can do on social media is very small and with no support from Facebook or other social networks and a general push back on the issues of IPR, it seems like the problem may be huge, but not calculable!

e) Four out of ten.

Q11. What in your experience are the scale and the characteristics of infringement of your IPR on social media?

a) Instagram and Twitter do not pose too much of a threat, however, as mentioned Facebook is used as a platform to sell on counterfeit goods. It is often difficult to locate this content because it appears in closed selling groups or hidden profiles, unavailable to the average user.

b) Mainly, social media users are ignorant of copyright and trademark law.

c) Increasingly prolific in the Far East. Problem is largely contained in Europe.

d) Don't understand the question.

e) Sales of fake products and pirated copyrighted material are rife but in closed selling groups. Posts are made all the time selling, using fake accounts or pages, which are moved and changed regularly. It is like whack-a-mole. Hard to catch the criminals without a lot of time and resources to investigate or even track down the criminals.

f) Six. (out of ten) Quite big and poor-quality goods.

Q12. Have you seen a rise in the infringement of your IPR over the past five years and to what do you attribute this, e.g. improved delivery mechanisms or new 'platforms'?

a) Infringement has slightly shifted in terms of where we find it. Mobile selling apps and social media are now hotbeds for counterfeit activity, whereas a couple of years ago marketplaces such as eBay were our target.

b) Yes, with the proliferation of SNS, auction and large selling sites (like Amazon) the IPR knowledge level of users is low and most do not read the site posting policies beforehand.

c) Impossible to tell. No data to inform comparison.

d) Yes, we have seen a very big rise on fake goods of our brand. Supply chain routes using social media and modern international delivery systems have increased the demand for counterfeit goods. Also, the economic downturn in Europe has placed pressure of staff cuts at customs borders and counterfeiting is now no #11 on their priority list.

e) It is about the same, just shifting platforms.

f) Yes there has been a rise. Reasons – lack of enforcement by police and Trading Standards. Lack of appropriate sentencing in courts. Ease of ordering online and through social media, unemployment.

8.2. Appendix 3: Enforcement Agency Survey Responses

8.2.1 IPO Intelligence Hub survey response

Q1. Current government enforcement activities and any changes in the last five years

The establishment and funding of the National Trading Standards Board (NTSB) in 2012 by BIS was supposed to create a network of intelligence analysts and a national intelligence hub, but it has not been effective. There are increased opportunities for raising awareness of the use of intellectual property rights interventions in disrupting organised crime groups (OCGs). The PIPCU funding from the IPO is seen by some in the Trading Standards (TS) world as misplaced and has led to resentment and disrupted partnership working. The current economic climate has resulted in a number of partnerships of necessity because of the cuts to services in many local authorities and police forces.

Q2. Differences in enforcing IPR in digital and physical goods

The IPO Intelligence Hub supports enforcement by gathering, analysing, developing and sharing intelligence. All intelligence is worked on, with no distinction made for physical versus digital goods.

Q3. Data collection on IPR infringements and differentiation on social media

Intelligence is received from the UK Border Force, Europol and Interpol, industry and brands, as well as the more traditional enforcement agencies such as Trading Standards and the police. There are regional differences in the level of intelligence submissions from Trading Standards. Crimestoppers is a very good source of IPR intelligence.

Q4. Work with other government agencies

There is little coordinated work undertaken in respect of social media as a result of the stance taken by the NTSB.

Q5. Scale and characteristics of IPR infringement on social media

Complaints are frequently made by rights holders and members of Trading Standards about the frequency of sales of counterfeit goods on social media sites. Because of the way the groups such as ‘closed groups’ are constructed, the viewing of goods by law enforcement or government staff requires a surveillance authority under the Regulation of Investigative Powers Act 2000. It is a relatively safe way for members of the public to trade.

Q6. Impact of social media on IPR infringement

The majority of the public in the UK see counterfeit goods as socially acceptable. There are sectors of society where this can and does translate beyond tolerance into actively seeking out counterfeit goods which have the appearance of luxury goods at a much more affordable price. Little thought is given to where the funds are going. In addition, social media governs many people's lives, so the use of platforms to trade is merely an extension of their routine social engagement.

Q7. Economic impact of social media on IP rights holders

The public tolerance of counterfeits, the ease of ordering via the internet and the relative security of anonymous online entities has created a safe haven for people to trade in counterfeit goods. This in turn has allowed an increase in trade. The counter-argument, however, is that those buying counterfeit luxury brands are unlikely to purchase the genuine article, so are not undermining the sales of genuine goods.

8.2.2. Trading Standards' eCrime unit

Interview

Trading Standards' (TS) eCrime unit, with a staff of just 12, acknowledges the problem of accurately measuring online commerce and illicit activity. They also recognise significant under-reporting of illicit activity, which means anecdotal evidence still dominates. We pointed out that our priority is to capture the trend in any data sets we are analysing, regardless of methodology, given how disparate the approaches adopted by the various agencies involved in enforcement are.

They mentioned that Citizens Advice (CA) handle complaints on 'scams' involving counterfeit goods and pass on the IPR-relevant cases to TS. The current data show an increase in IPR infringement on social media and the data are available in headline form. However, CA do not analyse the data in more depth and detail. There is an evident recent increase in online scams and this is prevalent on social media.

The EU are starting to work on online traffic and social media but it is clear that there is very little, if any, relevant data available, meaning our study could be the first to attempt to assess it. We explained the tripartite approach we are adopting using industry, government and consumer data to form a picture of what is going on.

They mentioned that the main tech firms expect to see claims made about the impact and losses supported by data, and acknowledged that Facebook's (FB) initial reaction was to ask for evidence. This is made all the more difficult as there is massive under-reporting of online crime, with a general observation that the amount of online crime is between five to ten times greater than what is actually officially reported.

They mentioned significant on-going challenges to getting and sharing data and that TS need to follow up on consumers' complaints. They work closely with the IPO's intelligence team and are involved in broader operations, such as the recent Operation Jasper. There is a belief that TS meets cynicism from consumers (when it comes to their justifying their purchases of counterfeit goods), but TS noted increased levels of what are described as 'innocent' purchases, such as cosmetics and toiletries.

Trading Standards survey response

Q1. Current government enforcement activities and any changes in the last five years

Until relatively recently, the TS response to IPR infringement on social media platforms has been quite patchy across the UK. Good practice and active enforcement work have been on a fairly limited scale. Issues include difficulty in identifying the 'owner' of a social media profile and social media platform operators providing very little (if any) information to enable successful identification and location of offenders. There has been recent coordinated action in relation to the sale of infringing goods on Facebook (Operation Jasper), led and coordinated by the National Trading Standards (NTS) eCrime Team. TS now have a procedure to refer infringing content to Facebook, that they feel can be removed, subject to meeting criteria. This is an opportunity to develop more powerful responses to a growing problem.

Q2. Differences between enforcing IPR in digital and in physical goods

TS's wider remit of tackling all forms of online consumer scams makes it impossible to accurately quantify the time spent investigating digital and physical IPR infringement. But it is clear that a far greater proportion of time is spent investigating physical IPR rather than digital infringement. TS's finite level of resources requires a focus on where the greatest consumer harm is occurring. Physical products are often associated with product safety issues; furthermore, all current intelligence and consumer complaints suggest that the sale of physical products significantly outweighs the sale of digital products, with clothing, fashion accessories and DVDs easily the biggest categories.

Q3. Data collection on IPR infringements and differentiation on social media

The TS data in relation to IPR infringement come from a variety of sources but the primary sources are consumer reports, through Citizens Advice and intelligence reports, by way of the IPO and either of the two Trading Standards intelligence systems (Memex and IDB). There is no current straightforward mechanism to differentiate infringement on social media from other forms of online infringement, so they have to conduct keyword searches against various intelligence/data sources to capture the social media-specific data.

Q4. Procedure applied towards IPR infringement on online services platforms

TS now have a formal procedure in place with Facebook, agreed after extensive consultation between the NTS eCrime Team and Facebook. This allows any TS officer to identify potentially infringing content. The content and profile details are documented on a standard form, then passed to the NTS eCrime team, as the single point of contact (SPoC) between TS and Facebook. The request is then sent directly to Facebook, assessed and the content removed and/or profile closed, as appropriate. TS are working towards a similar procedure for Instagram, as intelligence suggests that this platform is now used to 'advertise' IPR-infringing products.

Q5. Work with other government agencies

TS work extensively with other government agencies and industry bodies in efforts to tackle IPR infringement on social media. The recent Operation Jasper saw them work closely with the IPO, the Anti-Counterfeiting Group (ACG), the Federation Against Copyright Theft (FACT), the British Phonographic Industry and various brand representatives. They are members of the National Crime Agency (NCA)-led IP Operational Group. This group includes representatives from the National Police Chiefs Council (NPCC), the IPO, Border Force, customs and others. TS are also examining ways in which they can exploit the expertise developed by the police's IP Crime Unit (PIPCU) in terms of disruptive activities, such as the removal of merchant payment services and website takedowns.

Q6. Scale and characteristics of IPR infringement on social media

TS argue that it is difficult to accurately quantify the scale of IPR infringement on social media. This is for a variety of reasons – disparate recording of data and intelligence and low reporting levels being two of the primary reasons. In their experience, the types of online crime they investigate have reporting levels of somewhere between 5% and 10%. Factor in that IPR infringement generally has a lower reporting rate in any case and this makes it extremely difficult to fully understand the true nature of the problem.

However, the intelligence and data available do suggest that the sale of physical goods is the dominant factor. Taking a small sample of data in relation to Facebook specifically, clothing, fashion accessories and DVDs are the largest three categories, accounting for approximately 60%. The remaining 40% is made up of a mixture of footwear, electrical products, toys, toiletries and computer software. There is also evidence to suggest a strong link between the sale of IPR-infringing goods and the sale of illicit tobacco and alcohol.

Q7. Impact on social media of IPR infringement

The greatest impact (beyond the economic one) is that of consumer safety. Many of the products that were seized following Operation Jasper posed a significant risk to consumers.

Q8. Measuring increase in IPR infringement on social media

Using consumer complaints as one measure, Trading Standards has seen a marked increase in the scale of infringement on social media, which, since 2010, has shown a 400% increase in complaints attributed to Facebook, from around 1,300 complaints in 2010 to over 5,000 complaints in 2014. There has also been a corresponding increase in intelligence submissions onto either of the two Trading Standards intelligence systems. A sample of over 200 intelligence submissions from the northwest region showed that submissions on social media IPR infringements far exceed those on the sale of infringing products on eBay.

Q9. Economic impact of social media on IP rights holders

Given the significant (and on-going) increase in the use of social media to commit IPR infringement, there is little doubt that this is having a significant impact on IP rights holders, but TS are unable to properly quantify the impact. Social media is an attractive platform to use when 'advertising' IPR-infringing products, as there are no fees or costs but users are still able to find buyers/sellers in the local area. These combine to make social media an attractive proposition when compared to some of the more traditional marketplaces such as eBay, Amazon and Gumtree. Facebook is now second only to eBay in consumer complaints to Citizens Advice, with trends suggesting that Facebook will soon overtake eBay. Clearly this has an impact on legitimate traders, particularly at a local level. There is anecdotal evidence to suggest that independent retailers and smaller stallholders are directly affected by the ability of social media sellers to identify buyers on a local level.

Appendix 8.3 Technology Firms' Survey Responses

8.3.1 Google

The response to our questionnaire from Google, as of the end of August 2015, was to point us in the direction of their established code of practice in relation to online piracy. We informed them that this code only dealt with digital goods and responded by asking for their comments about the recent announcement that Bing had taken steps to alert consumers to the dangers of purchasing medicines online, and the likelihood that these could be both fake and dangerous. They subsequently sent us an official document that covered counterfeiting. Highlights are:

How Google fights the advertisement of counterfeit goods and Google's AdWords trademark policies

Over 1 million advertisers across 190 countries use AdWords – the majority of which are SMBs (small to medium-sized businesses). We allow trademarks to be used as keyword triggers in AdWords – for example, BMW running ads when someone searches- for 'Ford' – because people searching on Google benefit from being able to choose from a variety of competing advertisers. It is completely normal for a supermarket to stock different brands of cereal on the same shelf or for a magazine to run BMW ads opposite an article about Ford, so it does not make sense to limit competition online by restricting the number of choices

available to users. If a user is searching for information about a particular car, he or she will want more than just that car's website. They might be looking for different dealers that sell that car, for those who sell it second-hand, or for reviews about the car, or they may be looking for information about other cars in the same category. Providing users on Google with more than one option when they search for a brand name or other trademark helps them to find the best product at the lowest price.

We are not in a position to arbitrate trademark disputes all over the world and determining what is infringement is complex as it is a job for a judge, not us. Trademarks are territorial, apply only to certain goods or services, and often can be common words and phrases. That said, as a courtesy to brand holders, we do investigate reasonable claims about trademark violations in ads and we have found that this cooperation works well. They refer us to their specific region/country for their specific policies,[100] as well as easy-to-use complaint forms for trademark holders.[101]

And when it comes to advertising counterfeit goods, which is a very different situation, we have a zero-tolerance policy. As far as we can tell, people, generally, are not confused by seeing ads on searches for trademarked terms. If you look at the Google search results page, the ads are very clearly delineated as 'sponsored links', and ads that are actually deceptive would violate our Terms of Service (ToS). Using Google Insights for Search, it is clear that when people search for a trademarked term like 'Nike' or 'coke', they often also search for competitors either before or after, which suggests that they want to see information from more than one advertiser on these terms.

Thanks to the internet, it has never been easier to start a business and reach a huge audience. E-commerce services like eBay, Amazon and PriceMinister, advertising platforms like Google's AdWords and other online services help companies large and small operate at an incredible scale and empower consumers with more choices in the market. In the US alone, the ads-supported internet contributed $530 billion to the economy last year and 5.1 million jobs.

Unfortunately, a small percentage of bad actors misuse legitimate online services to try to sell counterfeit goods. For our part, we received legitimate complaints from a small fraction of 1% of advertisers in the last year.

Counterfeiting is not a new problem, of course. Just as with any new technology, the internet creates new complexities and many stakeholders have a role to play in resolving this issue. It is critical for brand owners and law enforcement to tackle counterfeiting at its source. Online services and other stakeholders can help, too. Although, it is important to remember that online services are in no position to determine the authenticity of the millions of advertised goods, as they never even take possession of them and fraudsters are always coming up with more sophisticated ways to play the system.

---

100 Google Ad Words Policy' [Online]: https://support.google.com/adwordspolicy/answer/6118?hl=en&rd=2
101 Google Trade Mark Complaint' [Online]: https://services.google.com/inquiry/aw_tmcomplaint

Clear policies and enforcement

We have clear policies against using AdWords to promote counterfeit goods. When abuse is brought to our attention, we act expeditiously on it, and we terminate accounts in appropriate circumstances.

Automated abuse detection

Ads that violate our policies can be tough to detect, as bad guys come up with new ways to cloak their behaviour all the time. To combat this, we look at thousands of data signals to automatically analyse every AdWords ad and account, and determine whether it is likely to violate our policies. Our systems are designed to examine a number of factors, including ad text, keywords and account characteristics (e.g. we might see if the current location matches the billing address). Depending on this examination, the ad and account will be subject to further manual review, or blocked entirely. No system is perfect, but we are constantly working to develop our advanced risk-modelling systems in order to address new threats. The system is designed to 'learn' from past instances of fraud and abuse – the more data the system has about past activity, the better it is about predicting abuse in the future.

Counterfeit reporting tools

The cooperation of brand owners is absolutely essential to our efforts. Even though our tools are state of the art, it is not always easy to spot a fraudster selling fakes. That is why we also rely on businesses to report feedback on advertisements themselves. If a counterfeit version of a product is being advertised via AdWords, a brand owner can notify us through a simple form and any users can report sites that violate our policies.

Law enforcement

To address illegal activity at its source, we support the enforcement of laws against counterfeiting and respond to appropriate legal process received from enforcement entities. Google regularly reports to a wide array of law-enforcement authorities, including working with officials to combat counterfeiting.

Collaborating with industry

Counterfeiting is an industry-wide issue, and we work with and support a number of industry groups that work together on enforcement strategy, knowledge sharing, training and networking, including the International Anti-Counterfeiting Coalition and the International Trademark Association.

Taking on counterfeits beyond ads

Along with our significant investment in preventing the advertisement of counterfeits, we take this issue seriously across our products and have clear policies in place. Our enforcement practices include:

- Responding to valid complaints regarding bad actors attempting to directly make money from counterfeit goods using AdSense, as well as commerce platforms like Offers, Shopping, Trusted Stores and Wallet.

- Responding to valid complaints about the sale or promotion of counterfeit goods through content that users host with us, including on Blogger, Google+, Sites and YouTube.

- Removing sites from Web Search based on valid court orders. Where a complainant has a court order adjudicating content on a particular page as unlawful, they can submit that through a simple form, and it is our policy to then remove that page.

8.3.2 Facebook

The information below represents a summary of comments made by Vick Baines (VB) to the IP Crime Group. VB is Facebook's Trust and Safety Manager, formerly in law enforcement, where she started as an Analyst in Surrey, subsequently working with Europol. She covers all crime across 127 countries and admits that collaboration between the technology industry and law enforcement is a sensitive subject.

Facebook's approach to IP crime

a) UK stakeholders have different approaches and these cover different crimes. Facebook's priorities are child exploitation, where they are "able to join the dots" when law enforcement is looking for evidence of criminality.

b) They have a real-name policy, which means users have to use their full legal name. Facebook is about trustbut VB noted that they are aware that law-enforcement agencies have set up fake accounts. They can and will close down these fake accounts.

c) Facebook prioritises whatever affects the safety of consumers, which means a focus on counter-exploitation and counter-terrorism. There is a diverse range of crimes that impact public safety and any criminal activity is against their Terms of Service.

d) Priorities are to all rights holders, but Facebook has to accommodate all the different laws and this requires individual notice procedure. They cannot assess bulk processing, although they can whitelist a trade body reporting for members and distinguish between © and TM infringements. VB claimed to have a turnaround response time of within two hours of receipt.

Law enforcement in the UK

a) VB usually deals with Trading Standards and does not encounter many involved stakeholders. The UK situation is complicated. Facebook reacts to allegations of infringement by producing a standard set of questions; sometimes they can have multiple requests, given the presence of multi-brand counterfeiters. There are issues regarding the proceeds of crime and on-going criminal investigations. Their existing takedown requests involve duplicates from rights holders and Trading Standards (with test purchases), and they do allow for reporting of an album of photos.

b) Facebook is primarily a communication platform and is not about transactions, so there is a clear need to establish the exact nature of the alleged infringement.

c) Data requests are controlled, meaning only accredited agencies can secure data. Facebook has agreements with the Home Office and the ICO to supply basic subscriber info, which has to come from their Dublin office. They approve 75% of communication data requests.

d) Facebook is a US firm and thus subject to US laws as far as divulging data is concerned. This means it takes six months to get the content of subscriber accounts, even though they can volunteer subscriber info. They need justification before providing data and pointed to the dedicated online data request form for sending details of crimes.

e) Facebook can provide the same information for Instagram, where they can see certain levels of infringement.

Questions/comments from IP Crime Group

a) Graham Moog from the ACG argued that the majority of users do not follow Facebook's terms and conditions. VB responded that these can be reported as fake accounts but the big issue is their refusal to accept bulk requests.

b) Dave Lowe from the IPO asked whether it is possible to adopt a more streamlined and coordinated approach. VB's response was that their IP lawyers are risk averse and cannot understand the fragmented approach to enforcement. They are keen to avoid independent regulators and, while it is clear that streamlining enforcement would improve processes, Facebook insists on proof.

c) John Alty from the IPO suggested reviewing international comparisons for good practices. It is clear that the diversity of stakeholders makes it harder for Facebook to manage and in other jurisdictions it is usually simpler, as in the case of alcohol in Sweden, which is more clearly regulated by the state.

Immediately subsequent to the IP Crime Group meeting, we contacted Facebook, and almost three months after sending a questionnaire relating to the use of social media platforms to sell counterfeit goods, we received the answer below. Essentially, it directed us to Facebook's

existing published policies and public positions.

"I fully appreciate that we may be far too late in sending you a response, but we'd like to contribute all the same. A number of colleagues worked on the following which, while not answering the questions exactly as you posed them, should go a fair way to provide you with the information you seek on our policies and procedures in relation to IP infringement. Facebook respects the intellectual property rights of others and is committed to helping third parties protect their rights. Our Statement of Rights and Responsibilities prohibits users from posting content that violates another party's intellectual property rights.[102] Our Help Center provides further information about intellectual property.[103]

"We offer tools for reporting infringing content that may be posted by users on our service. This includes Facebook's online reporting tool.[104] This tool can be used to report both copyright and trademark infringements. Upon receipt of a valid report of intellectual property infringement, we remove or block access to the reported content. In addition, in appropriate circumstances, we take further action against the accounts of repeat infringers, including removal of those accounts. The Electronic Frontier Foundation issued a report in 2014 describing aspects of our procedures.[105] Law-enforcement agencies may request data relating to a criminal investigation. Facebook discloses account records solely in accordance with its Terms of Service and applicable law. For more information, please see our law-enforcement guidelines[106] and Facebook's Data Policy.[107] Statistics on government requests for data and content removal are published every six months in Facebook's Government Requests Report."[108]

8.3.3 Twitter

Given the openly critical views expressed about online surveillance by Twitter's Nick Pickles (former head of Big Brother Watch), we were pleasantly surprised to receive a speedy and full response to the questionnaire where he said:

"Twitter will respond to reports of alleged copyright infringement, such as allegations concerning the unauthorized use of a copyrighted image as a profile photo, header photo or background, allegations concerning the unauthorized use of a copyrighted video or image uploaded through our media hosting services, or tweets containing links to allegedly infringing materials. Note that not all unauthorized uses of copyrighted materials are infringements (see our Fair Use page for more information).

"Twitter's response to notices of alleged copyright infringement may include the removal or restriction of access to allegedly infringing material. If we remove or restrict access to user

102 Facebook (2015) 'Statement of Rights and Responsibilities' [Online]: https://www.facebook.com/legal/terms
103 Facebook (2016) 'About Intellectual Property' [Online]: https://www.facebook.com/help/intellectual_property
104 Facebook 'Reporting a Violation or Infringement of Your Rights' [Online]: https://www.facebook.com/help/contact/208282075858952
105 Electronic Frontier Foundation (2014) [Online]: https://www.eff.org/pages/who-has-your-back-copyright-trademark-2014
106 Facebook (2016) 'Information for Law Enforcement Authorities' [Online]: https://www.facebook.com/safety/groups/law/guidelines/
107 Facebook (2016) 'Data Policy' [Online]: https://www.facebook.com/about/privacy/other
108 Facebook (2016) 'UK Government Requests for Data' [Online]: https://govtrequests.facebook.com/country/United%20Kingdom/

content in response to a notice of alleged infringement, Twitter will make a good-faith effort to contact the affected account holder with information concerning the removal or restriction of access, including a copy of the takedown notice, along with instructions for filing a counter-notification. In an effort to be as transparent as possible regarding the removal or restriction of access to user-posted content, we clearly mark withheld tweets and media to indicate to viewers when content has been withheld. We also send a copy of each DMCA notification and counter-notice that we process to Chilling Effects, where they are posted to a public-facing website (with personal information removed)."

Twitter has a specific policy relating to trademark infringement:

- Using a company or business name, logo, or other trademark-protected materials in a manner that may mislead or confuse others with regard to its brand or business affiliation may be considered a trademark policy violation.

- When we receive reports of trademark policy violations from holders of federal or international trademark registrations, we review the account and may take the following actions:

- When there is a clear intent to mislead others through the unauthorized use of a trademark, Twitter will suspend the account and notify the account holder. When we determine that an account appears to be confusing users but is not purposefully passing itself off as the trademarked good or service, we give the account holder an opportunity to clear up any potential confusion. We may also release a username for the trademark holder's active use.

- Twitter's counterfeit goods policy prohibits, but is not limited to, the following: products described as faux, replicas or imitations, etc., when referring to a brand name in an attempt to pass themselves off as products of the brand owner/other non-genuine products that attempt to pass themselves off as genuine products of the brand owner.

- Violations can be reported through our help centre. There are specific forms for copyright, trademark and counterfeit goods.

- Where content that violates our rules is brought to our attention, we will take appropriate action. As is standard industry practice, we do not proactively monitor the content user's post to Twitter.

The Twitter Transparency Report detailed the number of requests received by Twitter, both with regard to information requests from government agencies and copyright notices received. We noted that Twitter's 'Transparency Reports' on trademark notices for the six months ending 30 June 2015[109] and December 2015[110] both indicated that a relatively low number (6–11%) of accounts were affected by alleged trademark violations. Twitter noted in the most recent report that the number of trademark notices received for Twitter and Vine had declined by 33% (8,588 versus 12,911 in the previous January–June 2015 report).

Twitter stated that affected accounts were those "Twitter and Vine accounts where the account has been suspended in response to a valid trademark notice" and that each user was able to "remove or edit violating content after appealing account suspension". They also provided a number of reasons why they did not comply with every request, including:

- trademark notices filed by representatives who have not been authorised by the trademark owner;
- trademark notices that fail to provide sufficient information for us to locate accounts or material on Twitter and Vine;
- the large number of misfiled, non-trademark complaints through our web form;
- users may have challenged the notices after we have suspended them.

109 Twitter (2015) 'Trademark Transparency Report'. June 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jan-jun
110 Twitter (2016) 'Trademark Transparency Report'. December 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jul-dec

Appendix 4: Consumer Survey and Tracker Results and Analysis

Appendix 4.1: Definition of key terms used

The following are explanations of certain key terms used within the findings in the main report.

1. *Gini curve*. These charts are used to identify how distorted the distribution of any particular behaviour is across a population. Its most common application is in demonstrating that income is highly distorted towards a particular affluent segment of the population. The display on the vertical axis usually shows the distorted behaviour, e.g. the proportion of income, while the horizontal axis shows the proportion of the overall population. Thus, for income, the charts can display that the richest 10% have 31% of the income, the second richest segment have a further 15% of income, while the poorest deciles have 4% and 1.3% of the income respectively. We used the charts to illustrate how concentrated the promotion of suspect behaviour was, revealing that a small proportion of individuals, unique users, were responsible for a sizeable proportion of activity. For example, in Fig. A6.8b we can see that the top 20% of all eBay queries generated 10.8% of suspect results and 87.6% of branded results.

2. *Sankey charts*. These charts are used to visually represent the distribution of a multiple set of variables. The width of the lines connecting neighbouring bars represents the proportion of the population that share the two connected properties. By looking at Fig. A6.13a, we can see from the chart that a high proportion >50% of complicit purchases took place in branded online locations and over 70% of all their purchases were complicit in nature. A high proportion of these were driven by previous experience.

3. *Suspect behaviour*. This is a visual judgement of the nature of the material that a social media link refers to. The most common characteristic that distinguished these sites was the offer of a purchase at a substantial discount, at least 10% below the normal market price. In addition, some locations were explicit about these purchases being via alternative 'grey' channels, thus indicating that duty was being avoided. As can be seen, many of the locations provide a level of branding that infringed the trademark of the brand owner, as well as indicating the fraudulent behaviour of the purchase. Typically, the look and feel of these locations were somewhat amateurish and opportunistic and, in all likelihood, only the naïve would not notice the difference between these locations and the more sophisticated presentations used by authentic brand owners. However, this does not include fraudulent offerings that are virtually indistinguishable from branded sites. Such goods would require mystery shopping to identify the nature of the goods supplied.

4. *Website endpoints*. Digital communication is characterised by the prevalence of many different links between different messages. Materials are re-tweeted, affiliates recommend and followers are encouraged to click through. It is by its very nature a digital 'web' and this characteristic is particularly prevalent within social media communications. In contrast to these inter-connections, endpoints are those sites that facilitate actual transactions, rather than routing people elsewhere. They take orders, accept payments and execute instructions that will hopefully result in a delivery. Our study isolates these by looking at the route part of the URL internet address, e.g. www.ebay.com or www.facebook.com. It turned out that suspect activity was concentrated in a relatively small number of these endpoints distributed across the web.

5. *Communications*. In contrast to the endpoints, communications are typically short messages that advertise, promote or, in some other way, recommend following a link to other locations. Some of these links are shortened and re-routed via a host, having URLs like t.co/… or bit.ly/…. Sometimes, these just create links to other, typically longer, pages with information and blogs, but they also reach endpoints where transactions can take place.

Appendix 4.2: Gini curves of the distribution of exposure for the different search engines

The charts used (Figures A1 to A4) display the Gini curves for different types of behaviour. A Gini curve displays the proportion of an activity compared to the proportion of the population of initiators.

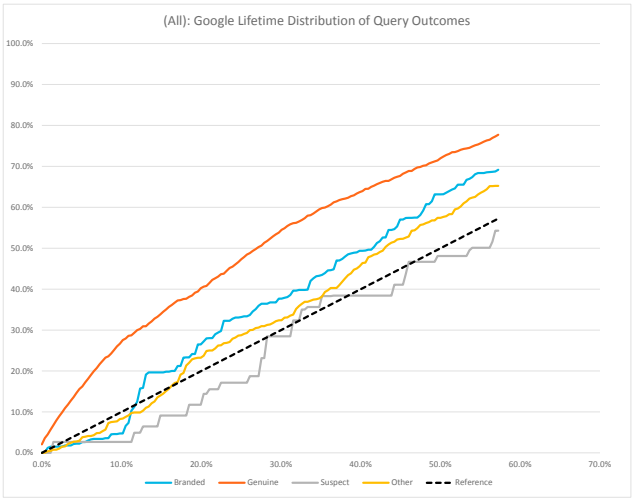


Figure A1 Gini curve of the distribution of the exposure of Google items by the proportion of initiators

The Google platform (Figure A1) kept the suspect behaviour distinct and diffuse from the other types of behaviour. This was illustrated by looking at the penetration of activities as the proportion of initiators grew. At the point of 20% of initiators, 11.8% of communications were 'suspect', in contrast to 39.4% of communications being 'genuine'.

The eBay platform (Figure A2) also demonstrated an even more diffuse distribution of suspect behaviour, at 20% of suspect initiators, 10.8% and 87.6% of communications were 'suspect' and 'branded' respectively.

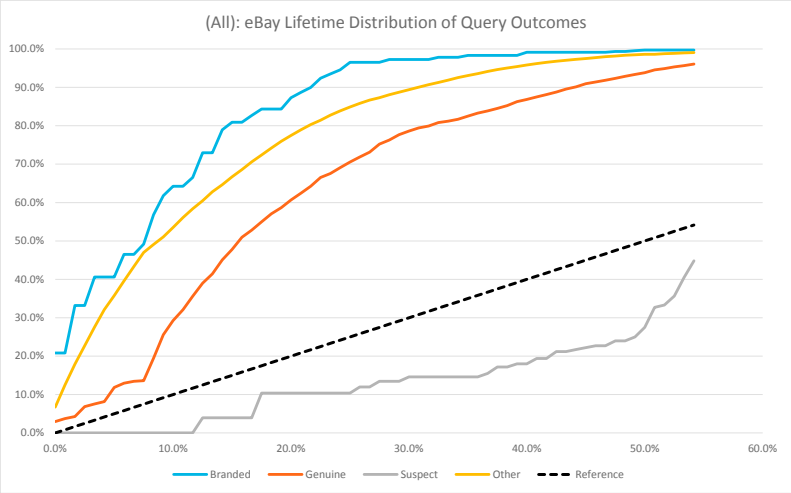


Figure A2 Gini curve of the distribution of the exposure of eBay items by the proportion of initiators

In contrast, the social media platforms (Figures A3 and A4) had highly concentrated suspect behaviour – within only 5% of initiators, 91.3% and 95.8% of communications were suspect and branded respectively.

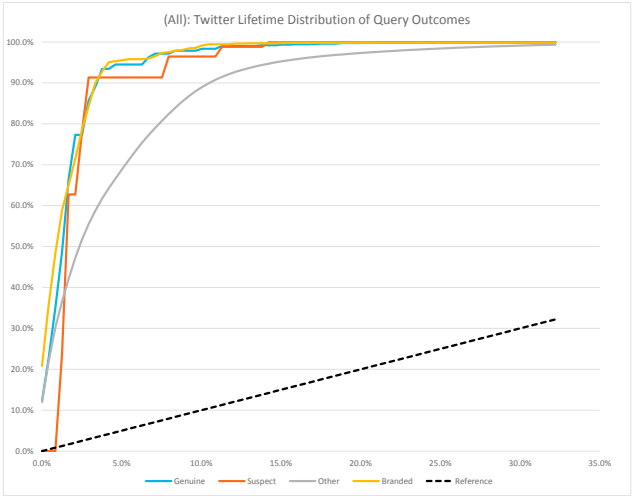


Figure A3 Gini curve of the distribution of the exposure of Twitter items by the proportion of initiators

Similarly, the behaviour within both types of group in Facebook was 72.1% and 84.3% of suspect behaviour within the first 20% of initiators for open and closed groups respectively.

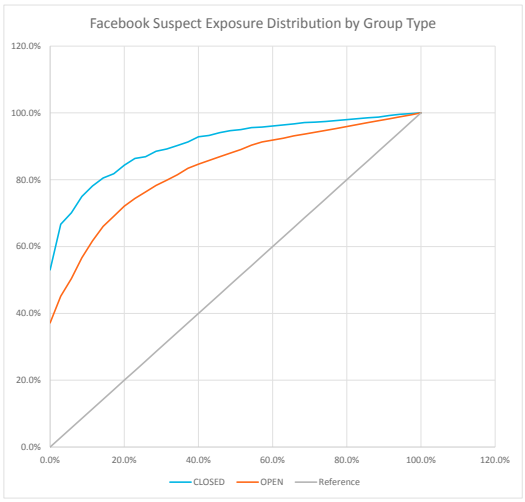


Figure A4 Gini curve of the distribution of the exposure of Facebook items by group type and proportion of initiators

One potential hangover from previous penetration of suspect behaviour arises within the footwear sector, where behaviour was found to be distinctly different from other broadcasts within eBay (see Figure A5 and Table A1). If we examine the distribution of eBay behaviours, suspect behaviour is mixed in with other types, with 20% of initiators driving 56.0% and 59.7% of suspect and genuine behaviours respectively.

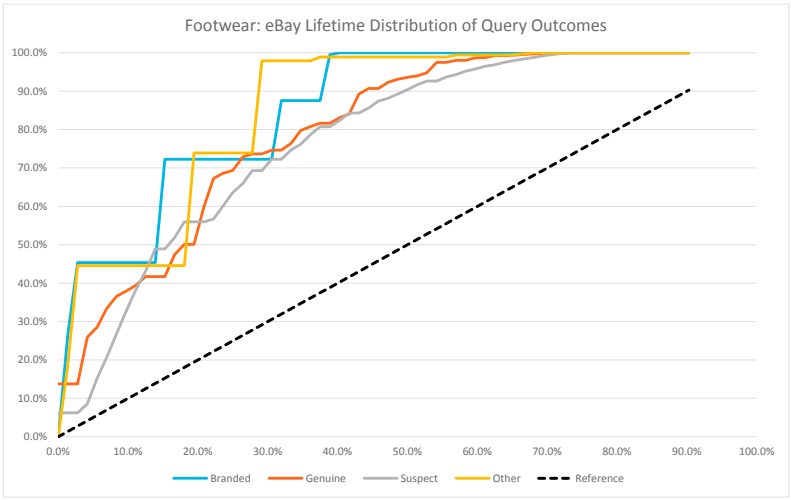


Figure A5 Gini curve of the distribution of the exposure of eBay items, for footwear brands alone, by the proportion of initiators

This contrasted with fewer outstanding differences for suspect behaviour within the other platforms as shown in Table A1.

Social Media Tracking (Footwear) 10% of Initiators	Branded	Genuine	Suspect	Other
Google	31.90%	36.80%	0.00%	11.90%
Twitter	98.50%	92.70%	99.50%	93.50%
eBay	45.40%	37.90%	32.70%	44.60%
Facebook (Open Groups)			96.00%	79.80%
Facebook (Closed Groups)			100.00%	98.90%

Table A1 The proportion of exposure within each online platform by content type, for footwear brands alone, from the most prolific 10% of initiators

Appendix 4.3: Consumer Survey Methodology

To capture the experience of consumers and how social media is used to make online purchases we designed a questionnaire which was conducted in July 2015. In conducting this survey, we first have to address three challenges: online sampling selection, verification of suspect online personas, and handling the highly skewed nature of typical digital behaviour.

Behavioural weighting

First, given our focus on the digital experience using social media or otherwise, online surveys were an ideal medium as they clearly and directly addressed the area of interest. However, it is well understood that online surveys are distributed among panels of people who have volunteered to participate. This self-selection presents a statistical challenge when endeavouring to use surveys to make general estimates of scale across the full range. On-going research by the British Population Survey (BPS) and others has demonstrated systematic differences between survey participants and those who merely transact online. These behavioural differences persist even after the demographic weighting that is normally applied as an online research correction is done. So, for example, panel participants are significantly more commercially and socially engaged, even if they are within the same age band and social grade as non-participants. The on-going offline tracking of research panel participants resulted in the calibration of a method of behavioural weighting. A series of questions, Q1 to Q4 were defined within the questionnaire that tested for the general levels of commercial behaviour and digital engagement to generate a weight to compensate for the typical over-engagement of research panel participants. This behavioural weighting was applied to all the results presented.

Categories of behaviour

Second, the study sought to explore the potential for consumers to participate in non-compliant behaviour. It was important to identify question wording that minimised the chance of steering or prejudicing any question response. To reduce the risk of sounding pejorative, we adopted the phrase ‘copied’ products. This particular word choice had the benefit of having been previously used,[111] as well as removing the sense that we were asking respondents to

111 Bryce, J. and Rutter, J. (2005) ‘Fake Nation – A Study into Everyday Crime’ [Online]: http://webarchive.nationalarchives.gov.uk/20140603093549/http://www.ipo.gov.uk/ipresearch-fake-2005.pdf

implicate themselves in anything deemed to be immoral and/or illegal.

The question used to define the different types of individuals is therefore worded as follows: "While making the purchase, did you consider the possibility that the products may be copies of products instead of genuine brands?" The potential responses offered were as follows:

Yes – but I purchased them anyway (a)
Yes – so I found another location (b)
No – but on receipt, I found that they did not appear genuine (c)
No – and on receipt they appear genuine (d)

We used response (a) to identify behaviour we labelled 'complicit' – those who knowingly participated in the market for copied products. We used response (b) to identify those we labelled 'compliant', and response (c) for those we labelled 'deceived'. For completeness, we labelled response (d) 'unexposed'. Based upon the classification of up to six different purchases, we segmented each consumer as follows:

(a) 'complicit' when at least one copied product was found and was still purchased – option (a), but no option (c);

(b) 'compliant' when once the copied product was found the purchase was made elsewhere – option (b), but no (a) or (c);

(c) 'deceived' when, at least once, products arrived that initially looked genuine but turned out to be suspect – any option (c);

(d) 'unexposed' when all purchases were themselves 'unexposed'.

That said, we were looking to identify behaviour that knowledgeable consumers would be aware was of marginal character. The nature of the subject may well have encouraged less straightforward participation. Online surveys may, in some contexts, benefit from being completed while the respondent is alone; if in company, respondents may well be less steered towards providing responses that they think any research worker would prefer. However, the very anonymity provides some opportunity for respondents to mask their true nature and in particular generate multiple personas. It can be seen as a cat and mouse game, as online technical skills can develop; for example, panels will restrict responses from particular internet protocol addresses, but services like The Onion Router (TOR)[112] enable these identifiers to be masked.

Within the data captured, there appeared to be a risk that this occurred at least once; a batch of 41 near-identical questionnaire responses occurred within a short space of time. These records were also in a section that was on the extreme end of online behaviour. To reduce the risk of these responses being over interpreted, the group of suspect duplicate responses was suppressed via a bootstrapping technique that weighted the responses, so that the suspect group was treated as a single response. Other responses from within the same demographic cell were re-sampled multiple times to form an alternative set of responses that were weighted

112 Software for enabling anonymous communication by hiding location or browsing habits of the respondent

to preserve the volume of the initial sample.

Structure and timing

Third, the study wanted to assess the distribution of behaviour online, and balance both the accuracy of specific responses with the opportunity to scale the behaviour. This led us to restrict exploration of purchases of specific products, instead addressing the last time a product was purchased. This kept the study synchronised with the online tracking study. Good questionnaire design is about focusing on specific incidents rather than asking consumers to make general assessments of typical behaviour. The structure of the questionnaire focused particularly on the last purchase within each sector and then asked how often this was done previously. The analysis was weighted on the assumption that each of the previous purchases had been conducted in the same manner as the purchase recorded. While this is unlikely to be strictly true for each individual, it is felt that this gives a reasonable sense of the scale of each type of behaviour that was prevalent.

The questionnaire was conducted during July 2015, the middle period of the online tracking study. The initial behavioural-weighting questions were asked of all participants and the survey was then filtered, based upon whether participants had made a transaction online within the specific sectors that are included in the study. The survey was concluded once 2,999 respondents had completed the study, with participants selected to match UK population demographic distribution (see Table A2). This selection demonstrated that the sectors we chose for the study had a slight gender bias (22% to 26% non-purchase for females to males respectively), and a larger age bias with age bands below 34 with a non-purchase rate of 15%, whereas the over 60s had a non-purchase rate in excess of 32%.

		At Least One Identified Purchase In the Last Year	No Tracked Purchases in last year.	Total
Gender	Male	1499	516	**2015**
	Female	1500	414	**1914**
Age	18-24	377	69	**446**
	25-29	405	74	**479**
	30-34	352	61	**413**
	35-39	216	47	**263**
	40-44	281	82	**363**
	45-49	344	99	**443**
	50-54	257	99	**356**
	55-59	297	123	**420**
	60-64	245	137	**382**
	65-69	129	93	**222**
	70+	96	46	**142**
Region	North East	154	37	**191**
	North West	277	100	**377**
	Yorkshire and The Humber	298	80	**378**
	East Midlands	129	82	**211**
	West Midlands	306	106	**412**
	East	288	112	**400**
	London	376	78	**454**
	South East	417	137	**554**
	South West	259	87	**346**
	Wales	154	39	**193**
	Scotland	252	58	**310**
	Northern Ireland	89	14	**103**
Social Grade	AB	833	210	**1043**
	C1	812	205	**1017**
	C2	582	160	**742**
	DE	772	355	**1127**
Total		**2999**	**930**	**3929**

Table A2 Comparison of the unweighted demographic distribution of respondents who had and had not purchased within the tracked consumer sectors

Characteristics of the study

With behavioural weights applied, it can be seen that the gender and age product biases were still clear. Detailed examination of the application of behavioural weights indicated that the highest weights were applied to those records with the lowest transaction frequencies. Overall, there was a 1.6% uplift compared to the higher frequencies. This was consistent with the general experience suggesting that online survey participants are more commercially engaged.

The average frequency was calculated for each individual by applying midpoint weights for each cell.

NUmber of Purchases in the last 12 months		Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times -12	Total	Ave. Frequency
Gender	Male	968	899	804	291	427	3389	3.72
	Female	804	903	864	345	483	3399	4.02
Age	18-24	214	220	224	93	126	877	4.05
	25-29	263	269	270	123	158	1083	4.1
	30-34	246	259	249	93	180	1027	4.28
	35-39	104	130	111	54	91	490	4.48
	40-44	153	151	169	52	94	619	4.06
	45-49	202	205	176	58	87	728	3.64
	50-54	139	151	133	55	61	539	3.7
	55-59	181	168	146	44	52	591	3.28
	60-64	136	141	92	32	35	436	3.14
	65-69	81	59	63	17	16	236	3.06
	70+	52	49	37	15	11	164	3.1
Region	North East	94	85	83	31	48	341	3.91
	North West	160	206	139	57	60	622	3.45
	Yorkshire and The Humber	167	172	164	54	87	644	3.85
	East Midlands	74	77	57	33	38	279	3.94
	West Midlands	193	194	172	72	75	706	3.61
	East	180	153	137	49	78	597	3.72
	London	213	218	286	99	204	1020	4.65
	South East	258	258	194	81	104	895	3.61
	South West	177	146	135	59	71	588	3.7
	Wales	72	98	103	25	42	340	3.81
	Scotland	138	153	147	50	77	565	3.91
	Northern Ireland	46	42	52	25	27	192	4.16
Social Grade	AB	478	530	548	195	340	2091	4.21
	C1	496	454	423	170	215	1758	3.74
	C2	346	376	300	126	163	1311	3.76
	DE	452	441	**398**	144	192	1627	3.67

Numerical frequency weights shown in brackets

Table A3 Comparison of the behavioural weighted demographic distribution of the claimed frequency of purchases within the tracked consumer sectors

Table A3, showed more frequent purchases online for the sectors visited by females, the highest volume of activity being within the age band 30–34, but the highest frequency of purchase being within the age band 35–39. There was also a preponderance of activity within the London region, marked by both higher volumes and higher frequency of purchase. It was also not surprising that those respondents within social grade AB (upper middle class/middle class) had a high capacity and frequency of purchase.

		Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times -12	Total	Ave. Frequency
Sector	Alcohol	111	115	178	96	304	804	6.51
	Cigarette	40	51	51	29	144	315	7.1
	Clothing	448	530	694	332	340	2344	4.34
	Footwear	521	632	443	97	58	1751	2.66
	Perfume	281	363	235	67	37	983	2.76
	Watch	371	112	68	14	28	593	2.12

Table A4 Distribution of claimed purchase frequency by consumer sector

As can be seen above (Table A4), the responses to the questionnaire indicated that purchases within the cigarettes sector were far more frequent than those within the watches sector, with 7.10 and 2.12 online purchases made per annum respectively. However, many more individuals made online purchases of clothing within the last year compared to cigarettes (2,344 to 315 respectively).

BRAND TYPES	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Sector Named Brands	290	520	462	163	272	1707	4.26
Other Brands	1482	1282	1207	473	638	5082	3.74

Table A5 Comparison of the distribution of claimed frequency by explicitly named sector-leading brands or other unnamed brands

The named brands within each consumer sector were based upon a comparison of the popularity of Google search terms. Consistent with this selection of the brands within each sector, the table above (Table A5) demonstrates the selected brands that were purchased at a level in excess of 13% above the unnamed brands (4.26 compared to 3.74 per annum).

Sources of Advice	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Everyday recommendations by a close friend or work colleague	260	309	310	135	228	1242	4.49
Advice from someone I only connect with via social media	100	192	161	68	155	676	4.95
Results of an online search for information	607	578	505	212	278	2180	3.78
Other sources of information online	324	298	299	124	194	1239	4.12
Previous purchases of the product from the same source.	702	913	966	380	668	3629	4.52

Table A6 Distribution of claimed purchase frequency by source of pre-purchase information

A comparison of the different sources of pre-purchase information (see Table A6) showed that while social media was the least common source of information for purchases, 676 (compared with 3,629) instances were decisions guided by previous experiences, and this was associated with the highest frequency of purchase (4.95).

Social Media Platforms Used	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Facebook	77	142	122	53	143	537	5.3
Twitter	40	90	79	37	138	384	6.23
Whatsapp	38	89	69	38	136	370	6.31
Google+	26	83	84	34	132	359	6.38
Instagram	13	59	64	35	128	299	7.09
Snapchat	7	50	46	24	131	258	7.74
Pintrest	8	44	46	18	120	236	7.69

Table A7 Distribution of claimed purchase frequency by social media platforms used

Where social media was used (see Table A7), it was evident that the average frequency of purchase increased in the opposite direction to the levels of use of a platform. Facebook had the highest level of use (537), but the lowest associated frequency (5.30), followed incrementally by Pinterest, with the lowest level of use (236) but the highest frequency (7.69). It became apparent that this divergence of frequency of purchase from frequency of use of a platform was a symptom of wider experience being associated with a wider repertoire of

platforms used.

LOCATION	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Online product branded website	295	320	254	99	88	1056	3.34
Online retail branded website	645	650	634	211	271	2411	3.64
Online unbranded site probably hosted abroad	24	66	60	22	41	213	4.7
Other online website	137	107	85	33	34	396	3.21
Online aggregation site (e.g. ebay, gumtree etc.)	206	206	163	63	51	689	3.21
Online Social Media site (e.g. Facebook, twitter etc.)	19	26	27	6	3	81	2.97
High Street Retail store	336	373	375	171	347	1602	4.79
Warehouse or other unbranded location	26	14	23	10	13	86	4.13
Market Stall	18	7	15	5	6	51	3.71
Informal Arrangement	5	5	2	2	2	16	3.69

Table A8 Distribution of claimed purchase frequency by ultimate location of purchase

While the study focused on online purchases, a substantial proportion (26.5%) still ended up with a purchase in a physical location, particularly a high-street retail store (see Table A8). It should also be noted that higher frequencies were associated with purchases knowingly connected with unbranded sites probably hosted abroad.

Whilst making the purchase, did you consider the possibility that the products may be copies of products instead of genuine brands?	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Yes - but I purchased them anyway.	218	251	249	82	161	961	4.22
Yes - so I found another location.	87	216	142	47	39	531	3.37
No - but on receipt, I found that they didn't appear genuine.	49	50	48	17	12	176	3.25
No – and on receipt they appear genuine.	1418	1286	1230	489	698	5121	3.88

Table A9 Distribution of claimed purchase frequency by attitude to provenance of products found

The vast majority of purchases made online, over 75%, appeared to be genuine (see Table A9). This proportion clearly may have included a proportion of undetected fraud but this was outside the scope of this study. It is also worth noting that, when considering financial harm, we did not recognise consequential activities: in particular, a purchase might be made on a suspect site but the product received turn out to be fine. However, accessing these sites might cause any device to be infected with detrimental software that can corrupt the device, detect subsequent activity, and/or capture financial and other sensitive information.

reasons for buying copied items	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Other family members wanted them	19	47	51	17	95	229	6.73
Could not afford otherwise	47	57	62	11	117	294	6.3
Lets me buy more	33	65	80	28	118	324	6.3
They are acceptable quality	68	94	89	32	127	410	5.61
They are much cheaper	77	113	104	39	124	457	5.27
Other	39	27	23	5	5	99	2.69

Table A10 Distribution of claimed frequency of purchase by motivation for purchasing copied items

Again, the most common responses were associated with the least frequent purchases (see Table A10). “They are much cheaper” had 457 responses (the largest), and an average frequency of 5.27 (the least). Looking at the response “Other family members wanted them”, which had the highest average frequency (6.73), indicated that there were hints of small-scale diffuse distribution networks within these complicit purchases.

reasons for not buying copied products	Once (1)	Twice (2)	3 to 4 times (3.5)	5 to 8 times (6.5)	Over 8 times (12)	Total	Ave. Frequency
Poor quality	29	76	59	23	24	211	3.91
I’d prefer the real thing	35	76	61	17	18	207	3.51
My family prefers the real thing	22	67	55	18	15	177	3.65
Products may be harmful	19	58	40	16	16	149	3.83
No guarantee	16	58	44	9	18	145	3.87
Links with organised crime	16	56	35	9	15	131	3.73
Other	13	48	40	14	13	128	3.88

Table A11 Distribution of claimed frequency of purchase by deterrent to purchasing copied items

Perhaps the most surprising finding drawn from the reasons not to purchase copied items was that there is a low level of perception of the risk of harm in these considerations; rather, the decisions to be compliant were more commonly selected as preferences (see Table A11).

After examination of the characteristics of different levels of exposure and responses to recent online purchases, it was worth breaking down the behaviour into the characteristics driven by the individuals concerned. To do this, we split the respondents into four segments in line with our overall definitions, as previously specified: ‘deceived’ individuals were those who acknowledged receiving any defective product via a past purchase from the selected sectors; ‘complicit’ individuals were those who were not surprised to receive a suspect product; ‘compliant’ individuals were those who only deferred when copied products were identified and only received good products; ‘unexposed’ had not acknowledged any copied product locations and only received good products from suppliers.

We can initially examine the demographic make-up of these different groups (see Table A12):

(%)	Complicit	Compliant	Deceived	Unexposed
Total	**18.0**	**6.0**	**4.8**	**71.2**
Male	19.6	6.6	6.2	67.6
Female	16.3	5.5	3.5	74.7
18-24	22.5	11.1	8.5	57.8
25-29	22.7	7.0	10.4	59.8
30-34	31.5	7.7	5.1	55.7
35-39	18.9	9.7	5.4	65.9
40-44	16.3	4.8	3.2	75.7
45-49	14.2	5.5	3.6	76.7
50-54	10.5	3.9	2.6	83.0
55-59	10.8	3.7	2.6	82.9
60-64	11.3	2.3	0.9	85.5
65-69	11.1	1.7	0.9	86.3
70+	9.3	2.3	1.2	87.2
North East	13.7	4.3	3.6	78.4
North West	17.1	4.4	3.2	75.4
Yorkshire and Himber	11.9	5.8	5.8	76.5
East Midlands	12.1	5.2	5.2	77.6
West Midlands	19.2	9.8	6.6	64.5
East	13.0	3.4	5.3	78.2
London	38.0	7.0	6.1	48.9
South East	13.1	5.0	3.9	78.1
South West	19.0	5.9	5.9	69.2
Wales	16.3	5.7	3.5	74.5
Scotland	12.2	7.4	2.2	78.2
Northern Ireland	25.6	8.5	6.1	59.8
AB	24.5	7.9	4.6	63.0
C1	13.0	4.7	3.6	78.7
C2	12.6	5.4	3.6	78.4
DE	19.9	6.1	7.2	66.8

Table A12 Demographic distribution of consumer segments based upon attitude to the provenance of products found online for purchase

Overall, just over 71% of respondents were ‘unexposed’ to the suspect locations or products, but this differs between different demographic groups (see Table A13). The highest proportions of ‘complicit’ behaviour occur within males, the age band 30–34, and social grades AB. There was also a suggestion that complicit behaviour is geographically concentrated within London.

As well as the differences in demographic, it was useful to differentiate behaviours:

LOCATION OF PURCHASE	Complicit	Compliant	Deceived	Unexposed
Online product branded website	18.00%	17.20%	16.80%	13.70%
Online retail branded website	36.60%	35.80%	23.60%	38.10%
Online unbranded site probably hosted abroad	10.90%	5.60%	7.90%	0.80%
Other online website	2.90%	2.50%	5.30%	7.00%
Online aggregation site (e.g. ebay, gumtree etc.)	11.50%	10.00%	12.60%	9.10%
Online Social Media site (e.g. Facebook, twitter etc.)	2.00%	4.20%	4.70%	0.20%
High Street Retail store	12.80%	20.60%	21.70%	26.70%
Warehouse or other unbranded location	1.70%	0.80%	1.70%	1.10%
Market Stall	1.10%	2.20%	3.80%	0.20%
Informal Arrangement	0.30%	0.30%	0.40%	0.20%

Table A13 Demographic distribution of consumer segments based upon attitude to the provenance of products found online for purchase

The strongest difference in locations (see Table A4.3l) was identified as the activity that takes place on unbranded sites probably hosted abroad. These sites presented clear risks for tracking, and also the complicit evasion of excise duty.

NUMBER SM Platforms USED	Complicit	Compliant	Deceived	Unexposed
0	13.90%	4.90%	3.40%	77.80%
1	29.60%	13.90%	15.70%	40.90%
2	32.10%	21.40%	25.00%	21.40%
3	46.50%	18.60%	11.60%	23.30%
4	51.20%	7.30%	12.20%	29.30%
5	54.30%	11.40%	11.40%	22.90%
6	50.00%	5.00%	20.00%	25.00%
7	74.50%	10.90%	5.50%	9.10%

Table A14 Distribution of consumer attitudinal segments by number of social media platforms used

The connection between social media engagement and ‘complicit’ behaviour is clearly shown in the table above (see Table A14). For individuals who did not use social media at all, the ‘complicit’ segment made up only 13.9% and the ‘unexposed’ were 77.8%. However, when all the suggested channels were acknowledged, the proportions were reversed, with 74.5% within the ‘complicit’ segment and 9.1% within the ‘unexposed’ segment.

This demonstrated that 'complicit' behaviour is symptomatic of high levels of digital engagement, as shown below (see Table A15), when the volume of purchasing is segmented.

ESTimated Net Target AnnUAL Transactions	Complicit	Compliant	Deceived	Unexposed
<= 2	13.10%	8.60%	2.50%	75.90%
3 – 11	17.40%	6.70%	4.80%	71.10%
12 – 21	19.70%	3.40%	6.30%	70.60%
22 – 31	19.50%	2.40%	6.50%	71.60%
32+	38.00%	5.00%	7.00%	50.00%

Table A15 Distribution of consumer attitudinal segments by est. total annual transactions within the tracked consumer sectors

If a respondent only acknowledged a low level of digital activity, they were much less likely to participate in complicit behaviour (13.1%), with over 75% within the unexposed segment, and the highest proportion of the compliant segment too. By contrast, when high levels of repeated purchases were conducted, the unexposed segment dropped to 50%, while the 'deceived' segment grew to 7.0% and the complicit segment reached 38%. This suggests that high levels of engagement with digital purchases are 'educating' individuals into more complicit behaviour, by teaching them the 'tricks of the trade' and potentially to source more material than is likely to be for their own consumption. It also looked like this exposure left them more susceptible to being deceived, probably because of the nature of the locations that are used.

The current study setup was unable to directly gain questionnaire responses from usernames identified within social media tracking. This would be an ideal extension of the study to invite questionnaire responses, particularly from those usernames that were doing high volumes of promotion. However, it was likely that completion rates would be low if an open invitation to participate were issued. At this stage, it was only possible to notice the similarities in behaviour from the different perspectives. This group of individuals, who participated frequently and were highly engaged with social media platforms, might overlap with those individuals that are generating the high volumes of outbound posts identified within the online tracking study. To demonstrate, we compared the distribution of behaviour across the different segments' estimated level of annual transaction activity (see Figure A6).

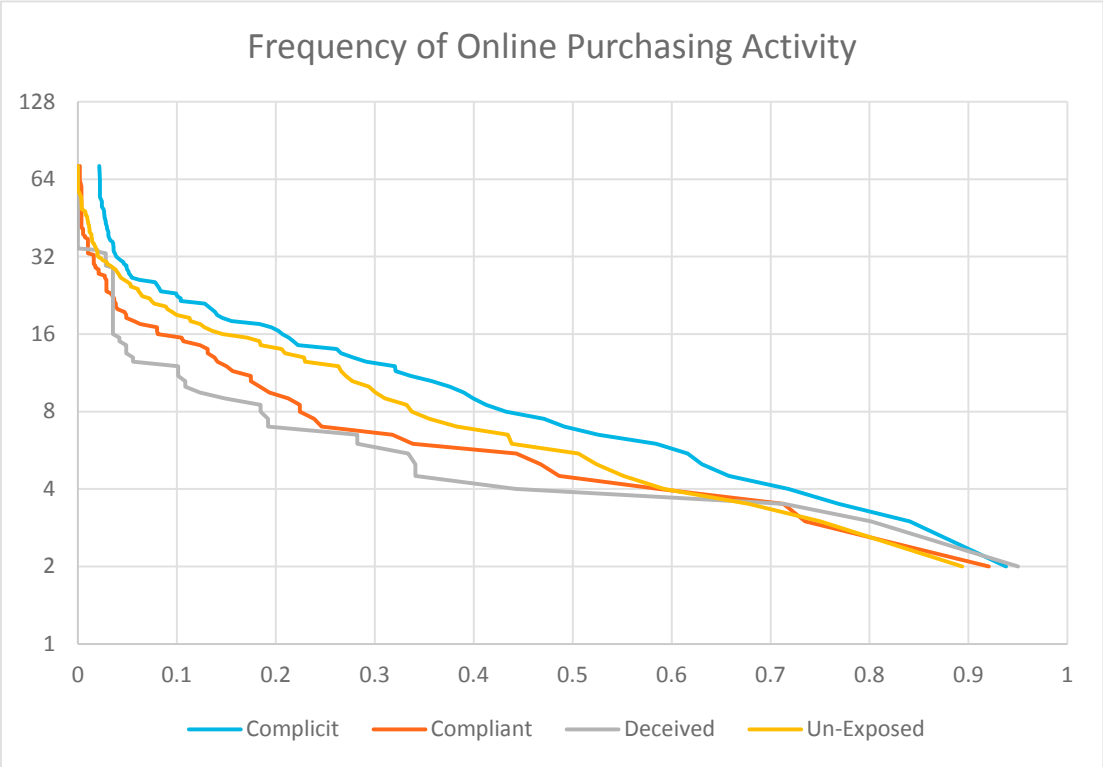


Figure A6 Net uplift in frequency of tracked purchasing activity by depth of population penetration, and by consumer attitude segment

The behavioural impact of social media

To investigate the characteristics of the segments visually across multiple axes, we used Sankey diagrams to visually display the weights of interaction between different variables. By comparing the width of the bands attached to each of the segment stages, we picked out the significant contribution to the complicit segment that arises from the opposite ends of the social grade groupings, AB and DE respectively (see Figure A7). In addition, high proportions arose within the younger age bands (18 to 29 and 30 to 39). By comparison, the deceived segment mostly consisted of those from the youngest age band and the lowest social grade alone.

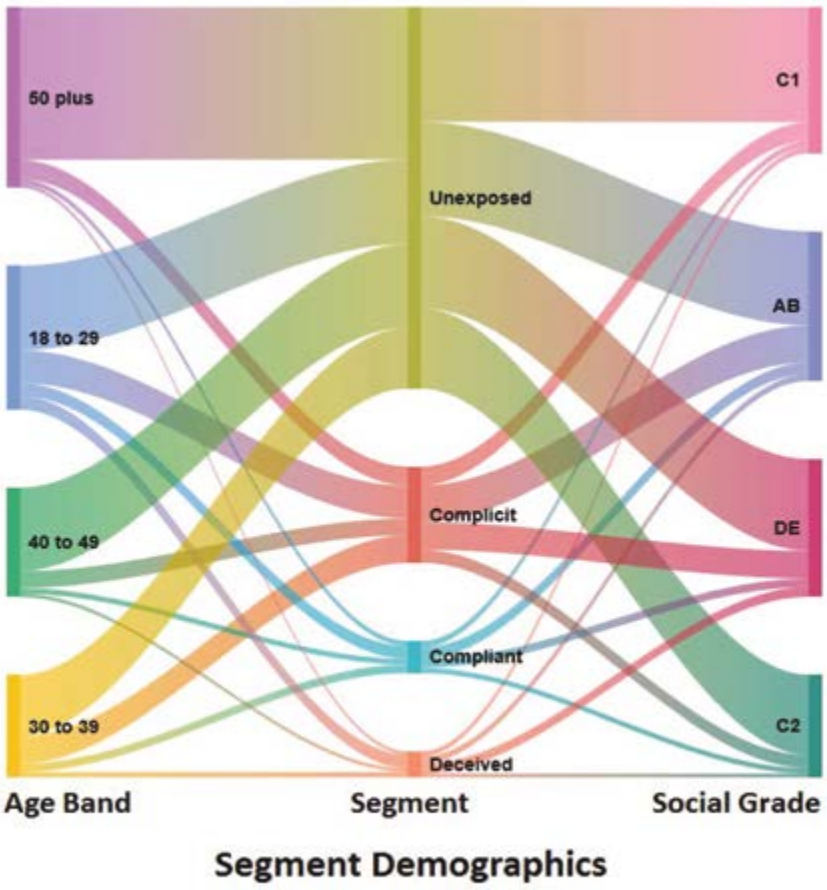


Figure A7 Sankey chart of the consumer attitude segments by key demographics, age band and social grade

There is no significance to the particular colours used within the Sankey charts other than to visually separate one band from another.

The following two charts demonstrate the differences in behaviour between the complicit segment and others.

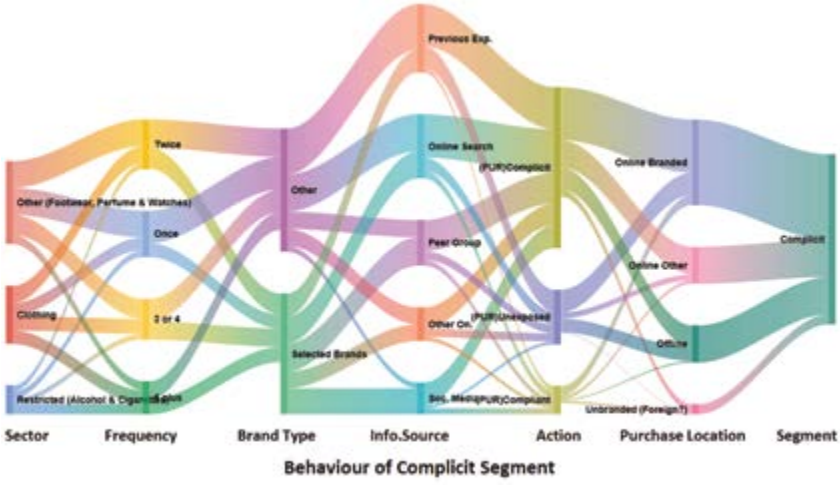


Figure A8 Sankey chart of the complicit segment by key online behaviours

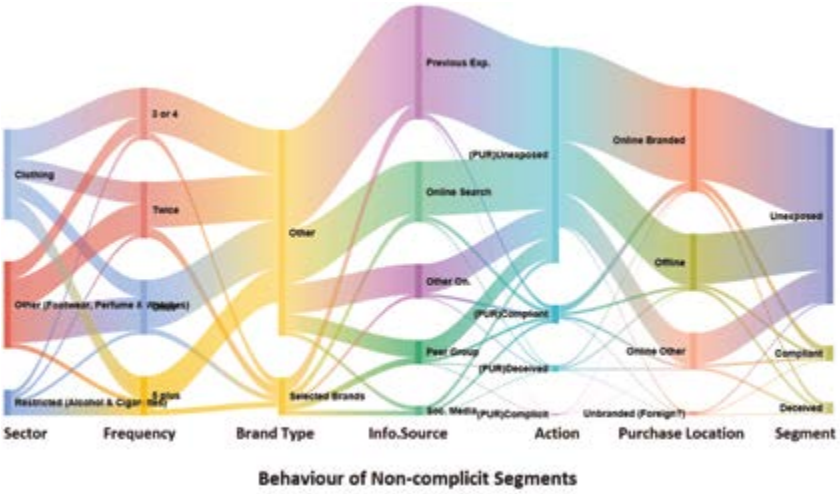


Figure A9 Sankey chart of the non-complicit segments by key online behaviours

The above two charts (Figure 8 and Figure 9) demonstrate the distinctive differences in behaviour. Complicit behaviour was easily discriminated and social media was the most common source of information, whereas for non-complicit behaviour previous experience was the strongest factor, with social media relegated to the least used information source. In addition, unbranded, possibly foreign, purchase locations were much more significant parts of the purchase journey for the complicit segment but were virtually absent from other segments.

Another interesting difference was that complicit behaviour was much more associated with sourcing popular brands, as indicated by the high proportion of connections with select brands within the research (rather than other un-referenced brands).

The final couple of charts focus explicitly on the contribution of social media, which lies at the heart of this study (see Figure 10 and Figure 11).

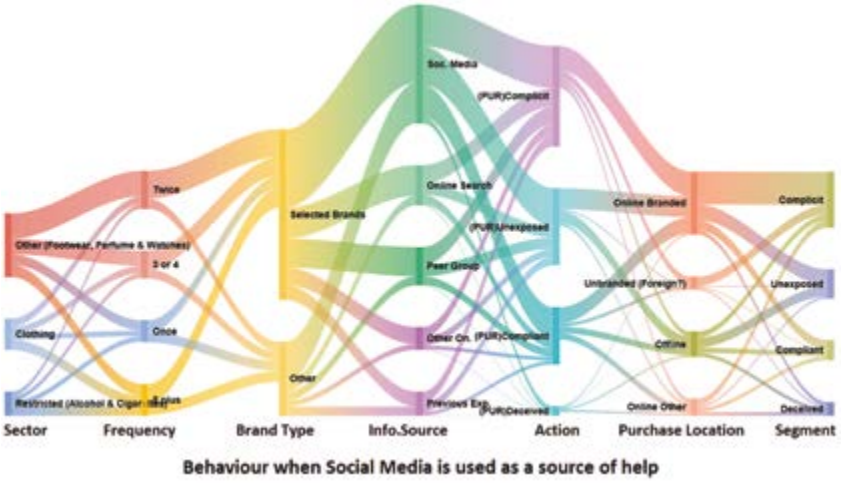


Figure A10 Sankey chart of the key online behaviours when mediated by social media

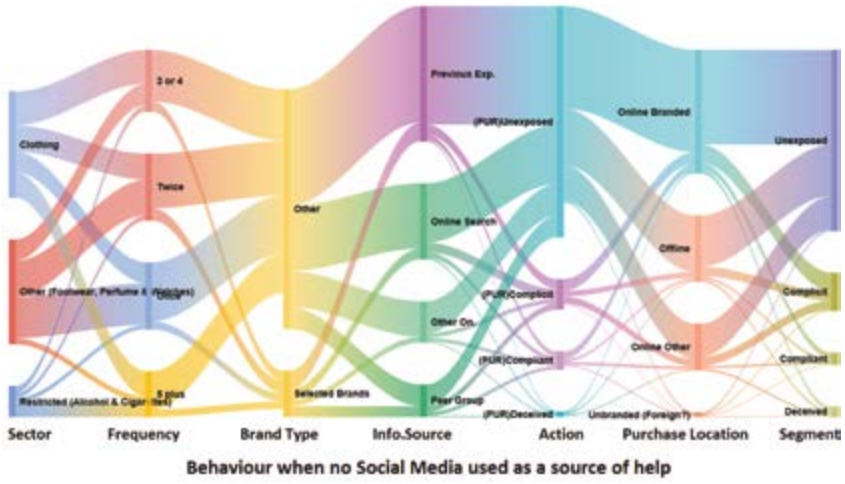


Figure A11 Sankey chart of the key online behaviours when no use of social media is acknowledged

When no social media was used, it appeared to be connected with dramatically different experiences. Firstly, the unexposed segment was by far the largest group, and unexposed individual actions were even more dominant. By contrast, when social media was used the

complicit segment was most prevalent, as well as the individual actions. Social media communications were much more closely associated with the promotion of unbranded, possibly foreign, hosts. Again, it was clear that the popular well-known brands were more associated with social media promotion. This suggested that complicit activity could be associated with further distribution, as the complicit behaviour was focused on popular brands that were sourced on the understanding that they were easier to pass on further.

In conclusion, from a variety of perspectives we see that the deliberate purchase of copied products formed a significant proportion (15.4%) of overall activity, at least within the sectors examined. Only 2.1% of purchases were estimated to be made as the result of deception. Social media had a significant contribution to this complicit behaviour, with 46.1% of complicit purchases involving social media, whereas only 4.1% of unexposed purchases involved social media.

Appendix 5 Other Economic Models and Approaches to measure the harm from counterfeiting

Alongside the GAO, Hopkins, OECD and BASCAP approaches covered in the main report we also considered other approaches to assessing social media's impact on modern consumer behaviour, including a review of behavioural economic literature and two models used to estimate deceived and complicit consumer behaviours.

Insights from behavioural economics approach

Recent books, like Richard Thaler's 2015 Misbehaving,[113] analyse consumer decision-making, noting underlying trends in consumer behaviour such as obsessions with discounts and "addiction to frequent sales". Thaler argues that there is an "endowment effect that all economic decisions are made through the lens of opportunity costs". Thaler describes his formulation of decision-making as involving acquisition utility (equivalent to consumer surplus) and transaction utility. The latter can be defined as "the difference between the price actually paid for the object and the price one would normally expect to pay", meaning it is about the quality of the deal.

Jordan Kasteler, writing[114] on social media's influences on behaviour, noted social media's influence on our shopping, relationships and education but raised the question of the role social media networking plays in the rest of our lives. He cited research suggesting that most social networks mainly support pre-existing social relations, suggesting that platforms like Facebook are used to maintain or strengthen existing offline relationships, as opposed to being used to meet new people. Social networks are often designed to be widely accessible but many attract homogeneous populations initially, making it easy to find groups using sites that are easily segmented. Citing Christakis and Fowler's Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives,[115] he explains the relationship between individuals and their networks of people, which either directly or indirectly influence their lives. Apparently, social networks can help spread contagions, create 'epidemics', disseminate fads and markets, alter voting patterns and more. He also describes social networks' ability to "harbor a flow of generally undesirable things such as anger and sadness, unhappiness, but good things also flow like happiness, love, altruism, and valuable information". He concludes that: "our own behavior, actions, and habits are likely to be largely more influenced and impacted by social media than we ever could have imagined".

113 Thaler, R. (2015) *Misbehaving – The Making of Behavioural Economics.* Allen Lane.
114 Kasteler, J. (2010) 'How Social Media is Influencing Your Behavior'. *Search Engine Land* [Online]: http://searchengineland.com/how-social-media-is-influencing-your-behavior-40615
115 Christakis, N. and Fowler, J. (2010) *The Surprising Power of Our Social Networks and How They Shape Our Lives.* Harper Press: London.

Christakis and Fowler also develop some useful concepts about the nature of groups, including group effects, self-organising groups and criminal behaviour, describing[116] how more connections within groups (known as a concentrated network) can reinforce behaviour in the groups, but more connections between groups (known as an integrated network) can open up a group to new behaviours and to behavioural change, for better or worse.[117] They also note that[118] in self-organising groups there are different outcomes between 'open' and 'closed' schools in terms of shaping attitudes. The changes in behaviour between the two beg the question of whether we can see appreciable differences between open and closed groups on social media platforms.

In relation to criminal behaviour,[119] they argue that even though "social networks are a valuable shared resource […] not all are in the best position to capture these benefits – [this] raises fundamental questions of justice and public policy". Even as social networks can be a "shared resource or public good",[120] they can function as "by-products of the actions of individuals acting with some self-interest". They have some relevant views on the way social networks function, not just for good but also as conduits for panic, and how they can be exploited for bad ends. They argue that "the interpersonal spread of criminal behaviour is an illuminating example of a bad network outcome" and claim that there is evidence suggesting that, partly because of social interactions, criminal actions in a given place and time will increase the likelihood that others will commit crimes, leading to more crimes occurring than would have been expected. And the groups over which these effects can extend can number in the hundreds.[121]

Estimates of economic impact of social media on sectoral revenue lost

This and the subsequent section use models to estimate the impact of social media on revenues generated in certain sectors and the drivers for complicit behaviour.

The first model used is based on 'Calculating the Effects of Counterfeiting Sales on Output, Total Revenue, and Profits of Legitimate Producers', which is cited without attribution in 'A review of the economic impact of counterfeiting'.[122] Their model assumes that counterfeiting reduces demand by competing with authentic legal offerings and that counterfeits are a perfect substitute for legitimate goods, meaning they are deceptive; as such, this implies that the model cannot be used for non-deceptive purchases. Given the argument from industry, as well as government and private enforcement agencies, that deception is made easier online because of counterfeiters' ability to employ authentic images and price items close to the genuine article, there is a clear sense that deceived purchases form a significant part of online trade. As such, the main impact of social media and other online platforms may well be an increase in the volume of deceived purchases and, accordingly, the model may still be useful in estimating the economic impact of such platforms on legal offerings.

116 Ibid., pages 116–117.
117 Ibid., page 117.
118 Ibid., pages 74–75.
119 Ibid., pages 294–95.
120 Ibid., page 292.
121 Ibid., page 294.
122 Spink, J. and Fejes, Z.L. (2012) 'A review of the economic impact of counterfeiting'. *International Journal of Comparative and Applied Criminal Justice,* Volume 36, Issue 4, 2012.

In order to relate the new results to the existing literature, we begin with the estimate of losses due to counterfeiting:

$$L_Q = R(1-R)\frac{Q_c^2}{Q_p} + Q_c$$

As mentioned several times elsewhere, the current examined research is inappropriate for making global estimates of the overall value of sales, but we can make some credible estimates of the relative effects of counterfeiting, particularly those from social media. As a result, rather than engaging in a detailed review of the applicability of this equation's assumptions when applied to the overall levels of equilibrium, we focus on the nature of the perturbations around an assumed equilibrium, wherever that equilibrium might finally land, once the deceptiveness (or otherwise) of counterfeits has been accommodated.

By concentrating on the relative effects, we can define a rate of change in counterfeit-based sales driven by changes in the level of social media, $\frac{\partial Q_c}{\partial S}$, where, formally, S relates to the level of social media activity.

We can derive a relative impact of counterfeit losses of:

$$\frac{L_Q}{Q_c} = R(1-R)\left[\frac{\partial Q_c}{\partial S}\right]^{-1}\frac{Q_c}{Q_p}$$

Currently, we lack detailed knowledge of the current profit margins within the respective markets we have studied, but the dependence on profit is maximal, $R(1-R) \leq 0.25$, therefore, it is straightforward to define an upper boundary on the

relative affects, while the research information provides us with independent estimates of the rates of counterfeiting relative to overall sales and the difference in counterfeiting rates relative to the absence of social media communications.

Applying this approach to the data captured within the online survey generates the estimates shown below (Table A16):

Sector	Counterfeit Rate (exc. Social Media)	Counterfeit Rate (inc. Social Media)	Social Media Rate Estimate ( )	Overall Counterfeit Rate ( )	Social Media Impact on Counterfeit Sector Revenue Loss
Alcohol	9.90%	67.10%	57.10%	14.90%	6.50%
Cigarette	14.30%	66.50%	52.20%	25.10%	12.00%
Clothing	9.00%	44.70%	35.70%	11.70%	8.20%
Footwear	12.10%	55.90%	43.90%	18.00%	10.30%
Perfume	20.40%	59.10%	38.80%	29.50%	19.00%
Watch	24.50%	64.60%	40.10%	37.10%	23.10%

Table A16 Sector estimates of the impact of social media on revenue loss due to counterfeit behaviour

Estimates of the drivers for complicit consumer behaviour

Once we have estimated the contribution from social media, we can also seek to understand the factors that lead to the generation of the complicit consumer behaviour we have seen in the existing research results. In this estimate, we sought to develop the conceptual model advocated by Chaudhry et al. The model is shown figuratively below (Figure A12):

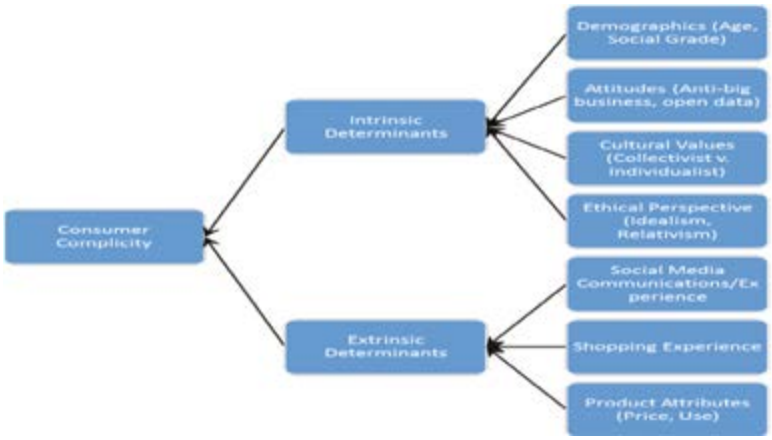


Fig A12 Conceptual model of consumer complicity – following Chaudhry and Stumpf (2007)

Source: Economics of Counterfeit Trade

The estimates were made using a stepwise linear regression across the research data, with the outcome variable, the consumer acknowledgement of complicity, assigned a unit score, +1. To help balance the model, those consumers who were unexposed to a counterfeit

experience were assigned a score of -1 – those exposed but not complicit were scored 0. Within the available predictor variables, data were initially summarised using a factor analysis to isolate out orthogonal variables to summarise the characteristics of different aspects of the schematic model. The model was split between extrinsic attributes, which are part of each individual's external environment, and intrinsic attributes, which relate to the individual's personal perspective.

Firstly, we need to define the extrinsic variables present within the captured research data as follows.

1. **Product attributes** were modelled by a linear combination of sector experience, the most discriminating variable, product difference (PD), which is orthogonal to the overall volume of activity. This is shown as:

$$PD = SP + SC\text{-}SA\text{-}SG$$

   Where SP is the presence of online perfume purchases, SC is the presence of online clothing purchases, SA is the presence of online alcohol purchases, and SG is the presence of online cigarette purchases.

2. **Shopping experience** was modelled based upon previous purchase experience, PE, the type of location of the final purchase, LC, plus a discriminating variable, SE, shown in the equation below of those relevant attributes that relate to experience within the purchase process that influences whether an individual is likely to make a purchase:

$$SE = PE + SD\text{-}PA\text{-}FR$$

   Where PE relates to the influence of previous experience, SD relates to sales discounts, PA relates to advice from professionals and FR relates to recommendations from famous people.

3. **Communications experience** was modelled using the combination of use of social media, SM, in online decisions and in addition the discrimination of the use of the internet, IS, claimed by each respondent:

$$IS = IE + IN\text{-}IO\text{-}ID$$

   Where IE is the use of internet for emails, IN is the use of the internet for non-grocery purchases, IO is the use of the internet for online dating and ID is the use of the internet to download movies.

The intrinsic variables have some straightforward elements:

1. **The demographics** present within the research included age, gender and estimated social grade (grouped into four levels: AB, C1, C2 and DE), which was estimated from declared occupation.

2. **Cultural values**, CV, were estimated from the influence of family and peers on purchase choices:

$$CV = CF + CC\text{-}CP\text{-}CO$$

   Where CF is the influence of friends and family, CC is the influence of reviews by other customers, CP is the influence of competitions, and CO is the influence of offers and vouchers delivered to home.

3. **Attitudes** were estimated from each respondent's current financial outlook, plus a discriminatory variable describing the purchases of discretionary products or otherwise, PD, of respondents:

$$PD = PL + PN\text{-}PC\text{-}PS$$

Where PL is the intention to purchase clothing, PN is the intention to purchase entertainment electronics, PC is the intention to purchase credit card services, and PS is the intention to purchase financial savings products. Along with these defined variables, a number of others were included, particularly those other sources of information at the point of online purchase. These variables were then added into an exploratory stepwise linear regression. The optimal result is shown in Table A17 below.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.886	0.015		60.495	0
SM	-0.097	0.017	-0.117	-5.605	0
PE	0.048	0.011	0.087	4.349	0
IS	0.025	0.007	0.075	3.597	0
SE	0.015	0.006	0.051	2.504	0.012

Table A17 Optimum stepwise regression model for complicit behaviour

Within the terms of the schematic model framework, the results suggest the dominance of extrinsic factors on the generation of complicit behaviour. These are the factors that show significant effects, as demonstrated by the Analysis of Variance ANOVA table shown in Table A18, and explain 21.5% of the variation. By comparing the mean square, it can be seen how influential social media experience is, with the impact of it more than three times greater than other effects. The social media (SM) mean square is 41.3 in comparison to 12.8 and 12.3 for the next-greatest influences, which are previous product experience (PE) and internet use (IS) respectively.

ANOVA							
			Unique Method				
			Sum of Squares	df	Mean Square	F	Sig.
	Main Effects	(Combined)	234.871	10	23.487	82.069	0
		SE	17.229	4	4.307	15.051	0
		IS	49.286	4	12.322	43.054	0
Complicit		PE	12.827	1	12.827	44.821	0
		SM	41.243	1	41.243	144.111	0
	Model		234.871	10	23.487	82.069	0
	Residual		855.128	2988	0.286		
	Total		**1089.999**	**2998**	**0.364**		

Table A18 ANOVA result for the optimum stepwise regression model

The summary effects of social media on counterfeiting using this model are shown below in Figures A13 (contribution to complicit behaviour) and A14 (impact on sectoral losses):

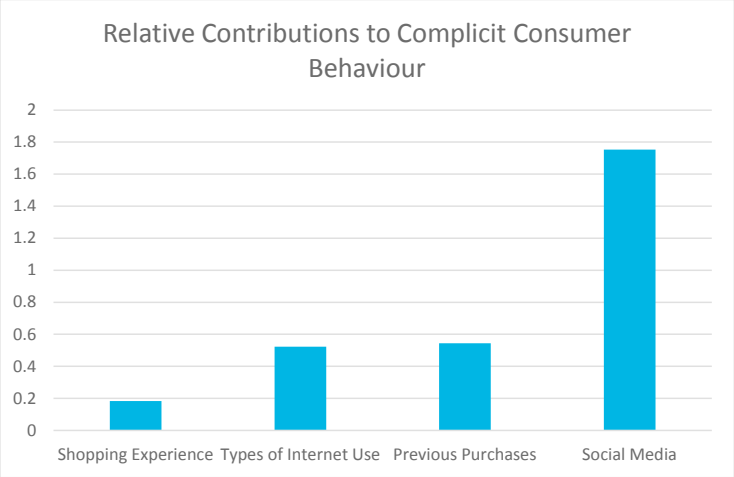


Figure A13: Relative significant contributions to the schematic model of complicit behaviour

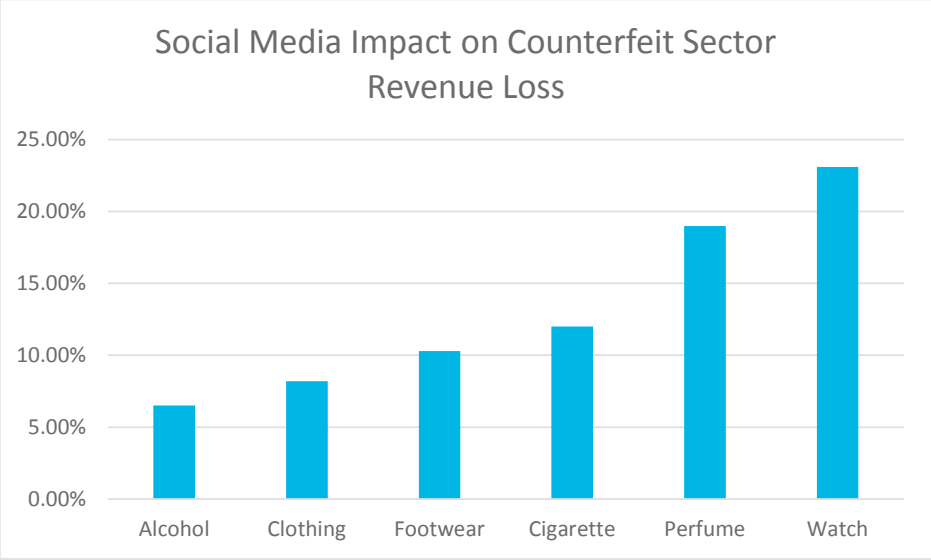


Figure A14: Sector-specific relative contribution of social media to the economic impact of counterfeiting

Appendix 8.6: Bibliography

Abutaleb, Y. and Maan, L. (2015) 'Facebook revenue, profit beat forecasts: shares hit all-time high'. *Reuters*, 4 November 2015 [Online]: http://www.reuters.com/article/2015/11/05/us-facebook-results-idUSKCN0ST2VF20151105

ACC/Spire Research and Consulting (2011) 'Counterfeits: Measuring it Fighting it' [Online]: http://www.slideshare.net/spireresearch/010216the-american-chamber-of-commercecounterfeit-measuring-it-fighting-it

Ahuja, A. (2016) 'What our digital social networks say about us'. *Financial Times*, 9 May 2016 [Online]: http://www.ft.com/cms/s/0/b6dcbee2-12b2-11e6-91da-096d89bd2173.html

Arthur, C. (2012) 'Google privacy policy slammed by EU data protection chiefs'. *The Guardian*, 16 October 2012 [Online]: http://www.theguardian.com/technology/2012/oct/16/google-privacy-policies-eu-data-protection

Arthur, C. (2014) 'Privacy campaigner Nick Pickles to become Twitter UK policy chief'. *The Guardian*, 1 May 2014 [Online]: https://www.theguardian.com/technology/2014/may/01/privacy-campaigner-nick-pickles-to-become-twitter-uk-policy-chief

Arthur, C. (2015) '"Safe harbour" ruling illustrates growing chasm between the US and EU'. *The Guardian*, *6* October 2015 [Online]: https://www.theguardian.com/technology/2015/oct/06/safe-harbour-ruling-growing-chasm-us-eu-data-protection

Bajpai, P. (2014) 'Why China is the World's Factory'. *Investopedia*, 22 October 2014 [Online]: http://www.investopedia.com/articles/investing/102214/why-china-worlds-factory.asp#ixzz3jvbq8gMw

Baraniuk, C. (2015) 'Tor launches anti-censorship Messenger' *BBC News* [Online]: http://www.bbc.co.uk/news/technology-34677323

Bartlett, J. (2014) *The Dark Net*. William Heinemann, London.

Basu, T. (2015) 'New Google Parent Company Drops "Don't Be Evil" Motto'. *Time Magazine* [Online]: http://time.com/4060575/alphabet-google-dont-be-evil

Bate, R. (2008) *Making a Killing: The Deadly implications of the Counterfeit Drug Trade*. AEI Press, Washington, USA.

BBC News (2015) 'Surveillance bill to include Internet records storage'. [Online]:http://www.bbc.co.uk/news/uk-politics-34715872

BBC News (2015) 'Details of UK website visits to be stored for year'. [Online]: http://www.bbc.co.uk/news/uk-politics-34715872

Big Brother Watch (2014) 'BBW Annual Review'. [Online]: https://www.bigbrotherwatch.org.uk

Billboard (2015) 'Europe's Top Court Throws U.S. Tech Firms for a Loop After Data-Sharing Pact Ruled Invalid'. [Online]: http://www.billboard.com/articles/business/6721791/europe-top-court-safe-harbor-pact-invalid-facebook

Billboard (2015) 'Cox Not Absolved From User Piracy'. [Online]: http://www.billboard.com/articles/business/6776939/judge-sides-with-bmg-and-round-hill-says-cox-not-absolved-from-user-piracy

Bing (2015) 'Bing to warn customers about the threats of fake online pharmacies'. 6 August 2015 [Online]: https://blogs.bing.com/search/2015/08/06/bing-to-warn-customers-about-the-threats-of-fake-online-pharmacies/

Blum, J. (2015) 'After Goldman Sachs is pirated, here are 10 of China's most audacious fakes'. *South China Morning Post,* 27 August 2015 [Online] http://www.scmp.com/news/china/society/article/1853159/fake-iwatches-salt-marijuana-and-starbucks-look-chinas

Blue, V. (2014) 'Google reverses "real names" policy, apologizes'. *Pulp Tech/ZDNet* [Online]: http://www.zdnet.com/article/google-reverses-real-names-policy-apologizes/

Brandwatch (2015) 'Amazing Social Media Statistics and Facts for 2016'. 7 March 2016 [Online]: https://www.brandwatch.com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016/

Bright, J. (2015) 'Intelligent Network Report: Facebook: Network and Technology Profile'. Ovum [Online] https://www.ovum.com/research/facebook-network-and-technology-profile/

Buchanan, W. (2015) 'What the Investigatory Powers Bill Will Mean for Your Internet Use'. *The Register*, 10 November 2015 [Online]: http://www.theregister.co.uk/2015/11/10/what_the_investigatory_powers_bill_will_mean_for_you_and_your_internet_use/

Bullas, J. (2015) 'Social media facts and statistics you should know in 2015' [Online]: http://www.jeffbullas.com/2015/04/08/33-social-media-facts-and-statistics-you-should-know-in-2015/

Burnham, K. (2014) 'Google+ policy change lets you mask your true identity with a pseudonym and allows you to make anonymous YouTube comments once again'. *Information Week*, [Online]: http://www.informationweek.com/software/social/google+-ends-ban-on-fake-names/d/d-id/1297336

Business Insider (2015) 'Epic slide deck from former Yahoo board member lays out the future of tech and media'. [Online]: http://uk.businessinsider.com/michael-wolf-predicts-what-will-happen-in-the-tech-industry-in-2016-2015-10?r=US&IR=T

Butler, S. (2015) 'Comscore's digital future in focus'. Butler Business & Media LLC, New York City [Online]: http://musicconfidential.biz/673.html

Bryce, J. and Rutter, J. (2005) 'Fake Nation – A Study into an Everyday Crime'. [Online]: http://webarchive.nationalarchives.gov.uk/20140603093549/http://www.ipo.gov.uk/ipresearch-fake-2005.pdf

Catsoulis, J. (2013) 'Narrow Space in Society, if Any, for Anonymity'. *The New York Times*, 11 July 2013 [Online]: http://www.nytimes.com/2013/07/12/movies/terms-and-conditions-may-apply-details-digital-age-loss-of-privacy.html?_r=1

Cellan-Jones, R. (2014) 'Social media told to simplify terms and conditions'. *BBC News* [Online]: http://www.bbc.co.uk/news/technology-30234789

Chaudhry, P.E. and Zimmerman, A. (2009) *The Economics of Counterfeit Trade: Governments, Consumers, Pirates and Intellectual Property Rights*. Springer Verlag, Berlin.

Chmielewski, D.C. (2013) 'Report links Google, Yahoo to Internet piracy sites'. *Los Angeles Times* 2 January 2013 [Online]: http://articles.latimes.com/2013/jan/02/entertainment/la-et-ct-piracy-ads-20130102

Chivers, C.J. (2016) 'Facebook Groups Act as Weapons Bazaars for Militias'. *The New York Times*, 7 April 2016 [Online]: http://www.nytimes.com/2016/04/07/world/middleeast/facebook-weapons-syria-libya-iraq.html?_r=0

Christakis, N. and Fowler, J. (2010) *The Surprising Power of Our Social Networks and How They Shape Our Lives.* Harper Press, London.

Cohen-Almagor, R. (2015) *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*. Cambridge University Press, New York, NY

Collopy, D., Bastian, V., Drye, T., Koempel, F., Lewis, D. and Jenner, P. (2014) 'Measuring Infringement Of Intellectual Property Rights'. [Online]: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/325020/IP_Measuring_Infringement.pdf

Coyle, D. (2016) 'The Sharing Economy in the UK'. [Online]: http://www.sharingeconomyuk.com/perch/resources/210116thesharingeconomyintheuktpdc.docx1111.docx-2.pdf

City Of London Police/Police Intellectual Property Crime Unit/PIPCU (2015) 'Fraud and Economic Crime'. [Online]: https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/About-PIPCU.aspx

Curtis, S. (2015) 'Wikipedia founder urges Apple to stop selling iPhones in UK if government bans encryption'. *Daily Telegraph* [Online]: http://www.telegraph.co.uk/technology/jimmy-wales/11974687/Wiki...o-stop-selling-iPhones-in-UK-if-government-bans-encryption.html

Danielson, T. and McAlone, N. (2015) 'Epic slide deck from former Yahoo board member lays out the future of tech and media'. *Business Insider* [Online]: http://uk.businessinsider.com/michael-wolf-predicts-what-will-happen-in-the-tech-industry-in-2016-2015-10?r=US&IR=T

DCMS (2015) 'Creative Industries: Focus on Employment (2015) by the Department for Culture Media & Sport'. https://www.gov.uk/government/statistics/creative-industries-2015-focus-on

DCMS (2015) 'Creative Industries: Focus on Exports (2015) by the Department for Culture Media & Sport'. https://www.gov.uk/government/statistics/creative-industries-2015-focus-on

Demos (2016) 'New Demos study reveals scale of social media misogyny'. [Online]: http://www.demos.co.uk/press-release/staggering-scale-of-social-media-misogyny-mapped-in-new-demos-study/

Dredge, S. (2016) 'Facebook gets its own Content ID with Rights Manager'. *MusicAlly*, 13 April 2016 [Online]: http://musically.com/2016/04/13/facebook-gets-its-own-content-id-with-rights-manager/

Drew, G. (2011) 'Etsy's social media DIY-saster'. *Salon.com* 15 March 2011 [Online]: http://www.salon.com/2011/03/15/etsy_privacy_people_search/

Duggan, M., Ellison, N.B., Lampe, C., Lenhart, A. and Madden, M. (2015) 'Social Media Update 2014: Demographics of Key Social Networking Platforms'. *Pew Research Centre* [Online]: http://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/

eBay (2015) 'Verified Rights Owners programme'. [Online]: http://pages.ebay.co.uk/vero/about.html

Economist (2015) 'The promise of the blockchain – the trust machine'. [Online]: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Economist (2016) 'The emporium strikes back'. [Online]: http://www.economist.com/news/business/21699103-platforms-are-futurebut-not-everyone-emporium-strikes-back

Economist (2016) 'How to win friends and influence people'. [Online]: http://www.economist.com/news/briefing/21696507-social-network-has-turned-itself-one-worlds-most-influential-technology-giants

Economist (2016) 'Regulating technology companies: Taming the beasts'. [Online]: http://www.economist.com/news/business/21699465-european-governments-are-not-alone-wondering-how-deal-digital-giants-taming

Electronic Frontier Foundation (2014) 'Who has your back? Protecting your speech from copyright and trademark bullies'. [Online]: https://www.eff.org/pages/who-has-your-back-copyright-trademark-2014

Electronic Frontier Foundation (2016) 'Terms of (Ab)Use'. [Online]: https://www.eff.org/issues/terms-of-abuse

Elliot, M. (2016) 'New numbers don't lie: counterfeits pose a growing threat'. *US Chamber of Commerce* [Online]: https://www.uschamber.com/op-ed/new-numbers-don-t-lie-counterfeits-pose-growing-threat

European Commission (2007) 'Counterfeiting Main Report'. [Online]: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/Counterfeiting_MainReport_Final.pdf.

European Commission (2010) 'Evaluation of the Intellectual Property Rights Enforcement Strategy in Third Countries'. [Online]: http://trade.ec.europa.eu/doclib/docs/2011/october/tradoc_148284.pdf

European Commission (2011) 'Commission Staff Working Paper: Impact Assessment on Proposal Regarding OHIM and European Observatory on Counterfeiting and Piracy'. [Online]: http://ec.europa.eu/internal_market/iprenforcement/docs/observatory/sec_2011_0612_en.pdf

European Commission (2014) 'Report on EU customs enforcement of intellectual property rights – Results at the EU border 2013'. [Online]: http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/2014_ipr_statistics_en.pdf

European Commission (2014) 'Internal Market IP Enforcement Action Plan'. [Online]: http://ec.europa.eu/internal_market/iprenforcement/docs/action-plan/140701-10-actions_en.pdf

European Commission (2015) 'Taxation and Customs Union -IPR Infringements: Facts and figures'. [Online]: http://ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/statistics/index_en.html

European Union Intellectual Property Office (2016) 'The Economic Cost of IPR Infringement in the Recorded Music Industry'. [Online]: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_music

European Union Intellectual Property Office (2016) 'Intellectual Property and Youth Scoreboard'. [Online]: https://euipo.europa.eu/ohimportal/en/web/observatory/ip-youth-scoreboard?platform=hootsuite

Facebook (2016) 'United Kingdom Requests for Data July–December 2015'. [Online]: https://govtrequests.facebook.com/country/United%20Kingdom/

Facebook (2015) 'Statement of Rights and Responsibilities'. [Online]: https://www.facebook.com/legal/terms

Facebook (2016) 'About Intellectual Property'. [Online]: https://www.facebook.com/help/intellectual_property

Facebook (2016) 'Reporting a Violation or Infringement of Your Rights'. [Online]: https://www.facebook.com/help/contact/208282075858952

Facebook (2016) 'Information for Law Enforcement Authorities'. [Online]: https://www.facebook.com/safety/groups/law/guidelines/

Facebook (2016) 'Data Policy'. [Online]: https://www.facebook.com/about/privacy/other

Facebook (2016) 'UK Government Requests for Data'. [Online]: https://govtrequests.facebook.com/country/United%20Kingdom/.

Felsted, A. (2015) 'Retail enters third phase of digital evolution'. *Financial Times* [Online]: http://www.ft.com/cms/s/2/e4ca5a7a-70ba-11e5-9b9e-690fdae72044.html

Flanagan, A. (2015) 'Facebook Announces New "Music Stories" Feature'. *Billboard* [Online]: http://www.billboard.com/articles/business/6753128/facebook-music-stories-feature-spotify-apple-music

Friedmann, D. (2015) *'Trademarks and Social Media – Towards Algorithmic Justice'. Edward Elgar Publishing*, Cheltenham, UK

Fuller, S. (2016) 'Can we win the war against the counterfeiters?'. *The Trademark Lawyer*, Issue 2, 2016, pages 36–38. CTC Legal Media [Online]: http://edition.pagesuite-professional.co.uk//launch.aspx?pbid=8f450367-5863-4898-9c66-eb82480402b1&pnum=42

Galam, S. and Vignes, A. (2003) *Fashion, Creativity and Efficiency: An Application From Physics*. Pages 11–12. Paris Center for Law and Economics. [Online]: https://www.researchgate.net/publication/5014534_Fashion_Creativity_and_Efficiency_An_application_from_Physics

GIPC/US Chamber of Commerce (2016) '*Measuring the Magnitude of Global Counterfeiting: Creation of a Contemporary Global Measure of Physical Counterfeiting'*. [Online] http://www.theglobalipcenter.com/wp-content/themes/gipc/map-index/assets/pdf/2016/GlobalCounterfeiting_Report.pdf

Global Web Index (2016) 'Internet users have average of 5.54 social media accounts'. [Online]: http://www.globalwebindex.net/blog/internet-users-have-average-of-5-social-media-accounts

Page L. (2015) 'Alphabet Investor Relations'. [Online]: https://abc.xyz/investor/founders-letters/2015/

Google (2015) 'Advertising Policies Help – Trademarks'. [Online]: https://support.google.com/adwordspolicy/answer/6118?hl=en&rd=2

Google (2015) 'Google AdWordsTrade Mark Complaint'. [Online]: https://services.google.com/inquiry/aw_tmcomplaint

Greenslade, R. (2016) 'Make Google and Facebook pay levy to support journalism – academic'. *The Guardian*, 26 May 2016 [Online]: https://www.theguardian.com/media/greenslade/2016/may/26/make-google-and-facebook-pay-levy-to-support-journalism-academic

Griffin, A. (2015) 'Facebook "Most Used Words" game is collecting huge amounts of user data, can sell it to whoever it wants'. *The Independent*, 25 November 2015 [Online]: http://www.independent.co.uk/life-style/gadgets-and-tech/news/fa...uge-amounts-of-user-data-can-sell-it-to-whoever-it-a6746791.html

Hann, G. (2015) *Tech and media predictions for 2016*. Taylor Wessing, Lexology.

Hoback, C. (2013) Terms and Conditions May Apply [Online]: http://tacma.net

Hopkins, D.M., Kontik, L.T. and Turnage, M.T. (2003) *Counterfeiting Exposed – Protecting Your Brand and Customers*. John Wiley & Sons, Hoboken, NJ

I am a Social Entrepreneur (2015) 'What Is Social Responsibility?'. [Online]: http://www.imasocialentrepreneur.com/social-responsibility/

Ingham, T. (2015) 'Facebook has 10 times as many users as Spotify and Pandora combined'. *Music Business Worldwide* [Online]: http://www.musicbusinessworldwide.com/facebook-has-10-times-as-many-users-as-spotify-and-pandora-combined/

The Inquirer (2014) 'Twitter appoints Big Brother Watch director Nick Pickles as UK policy chief'. [Online]: http://www.theinquirer.net/inquirer/news/2342668/twitter-appoints-big-brother-watch-director-nick-pickles-as-uk-policy-chief#

Interpol (2014) 'Harnessing global efforts against counterfeiting and illicit trade focus of international conference'. [Online]: http://www.interpol.int/News-and-media/News/2014/N2014-180

Interpol (2015) 'Interpol host global music industry anti-piracy conference'. [Online]: http://www.interpol.int/News-and-media/News/2015/N2015-028

ITV News (2015) 'Scam tricks Facebook users into hacking themselves'. 30 July 2015 [Online]: http://www.itv.com/news/central/2015-07-30/scam-tricks-facebook-users-into-hacking-themselves/

IACC (International Anti-Counterfeiting Coalition) (2016)'Counterfeiting Statistics'. [Online]: http://www.iacc.org/resources/about/statistics

ICC/BASCAP (2011) 'Estimating the global economic and social impacts of counterfeiting and piracy'. February 2011 [Online]: https://iccwbo.org/publication/estimating-global-economic-social-impacts-counterfeiting-piracy-2011/

ICC/BASCAP (2009) 'The Impact of Counterfeiting on Governments and Consumers'.

ICC/BASCAP (2009) 'International Engagement and Advocacy/Roles and Responsibilities of Intermediaries'. [Online]: http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and- Advocacy/Roles-and-Responsibilities-of-Intermediaries/

IP Front Line (2014) 'Counterfeit goods in social networks'. 26 November 2014 [Online]: http://ipfrontline.com/2014/11/counterfeit-goods-in-social-networks/

IPO (2014) 'IP Crime 2013/14 Report'. [Online]: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374283/ipcreport13.PDF

IPO (2015) 'IP Crime Report 2014/15'. [Online]: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/461792/ip-crime-report-2014-15.pdf

IPR Center (2016) 'About us'. [Online]: https://www.iprcenter.gov/about-us

Johnson, L. (2015) 'Animal Spirits: Silicon Valley's robber barons want to devour us'. *Sunday Times*, 22 November 2015 [Online]: http://www.thesundaytimes.co.uk/sto/business/Tech_and_Media/article1635450.ece

Kasteler, J. (2010) 'How Social Media is Influencing Your Behavior'. *Search Engine Land* [Online]: http://searchengineland.com/how-social-media-is-influencing-your-behavior-40615

Kohlmann, E. (2015) '27th January 2015 Testimony to the House Committee on Foreign Affairs Subcommittee on Terrorism, Non-proliferation, and Trade – "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media" – Charlie Hebdo and the Jihadi Online Network: Assessing the Role of American Commercial Social Media Platforms', Washington D.C.[Online]: http://docs.house.gov/meetings/FA/FA18/20150127/102855/HHRG-114-FA18-Wstate-KohlmannE-20150127.pdf

KPMG (2005) 'Managing the Risks of Counterfeiting in the Information Technology Industry'. [Online]: http://www.agmaglobal.org/cms/uploads/whitePapers/KPMG-AGMA_ManagingRiskWhitePaper_V5.pdf

KPMG (2014) 'Counterfeit Christmas: consumers risk buying turkeys instead of golden goose'. [Online]: http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublication...s-risk-buying-turkeys-instead-of-a-golden-goose-says-KPMG.aspx

Kuchler, H. and Garrahan, M. (2016) 'Does Facebook bend the trends that govern our news?'. *Financial Times* [Online]: http://www.ft.com/cms/s/0/5c68e88e-18e6-11e6-bb7d-ee563a5a1cc1.html

Kuchler, H. (2016) 'Facebook algorithm shift hits media groups'. *Financial Times* [Online]: http://www.ft.com/cms/s/0/28cfe2a6-28eb-11e6-8b18-91555f2f4fde.html?siteedition=uk

Laville, S., Wong, J.C. and Hunt, E. (2016) 'The women abandoned to their online abusers'. *The Guardian*, 11 April 2016 [Online]: https://www.theguardian.com/technology/2016/apr/11/women-online-abuse-threat-racist

Laville, S. (2016) 'Top tech firms urged to step up online abuse fightback'. *The Guardian*, 11 April 2016 [Online]: https://www.theguardian.com/technology/2016/apr/11/facebook-twitter-google-urged-to-step-up-online-abuse-fightback

Lawson, C. (2015) 'Online chatting at work gets the thumbs up from bosses'. *BBC News*, 27 November 2015 [Online]: http://www.bbc.co.uk/news/business-34911118

Lee, Y. (2015) 'China's "fake" Apple stores thrive ahead of new iPhone launch'. *Reuters*, 23 September 2015 [Online]: http://www.reuters.com/article/2015/09/24/us-apple-china-idUSKCN0RN2EF20150924

Lepido, D. (2014) 'Fakebook: Site Touts Luxury Goods That May Not Be What They Seem'. *Bloomberg,* 13 November 2014 [Online]: www.bloomberg.com/news/2014-11-13/fake-out-many-luxury-items-advertised-on-facebook-are-phony-researchers-say.html

Levy, A. (2016) 'Amazon's Chinese counterfeit problem is getting worse'. *CNBC* 8 July 2016 [Online]: http://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html

Lewis, P. (2015) 'Anti-Counterfeiting Group: fighting the good fight'. *Trademarks and Brands Online* [Online] http://www.trademarksandbrandsonline.com/article/anti-counterfeiting-group-fighting-the-good-fight

Lomas, N. (2015) 'Facebook, Google, Twitter Commit To Hate Speech Action In Germany'. *TechCrunch* 16 December 2015 [Online]: http://techcrunch.com/2015/12/16/germany-fights-hate-speech-on-social-media/

Lomas, N. (2016) 'UK study quantifies Twitter's misogyny problem'. *TechCrunch* 26 May 2016 [Online]: http://techcrunch.com/2016/05/26/uk-study-quantifies-twitters-misogyny-problem/?ncid=rss

Madrigal, A.C. (2012) 'Dark Social: We Have the Whole History of the Web Wrong'. *The Atlantic* 12 October 2012 [Online]: http://www.theatlantic.com/technology/archive/2012/10/dark-social-we-have-the-whole-history-of-the-web-wrong/263523/

Mander, J. (2016) 'Internet users have average of 5.54 social media accounts'. *Global Web Index* [Online]: http://www.globalwebindex.net/blog/internet-users-have-average-of-5-social-media-accounts

Margalit, L. (2016) 'The Psychology Behind Social Media Interactions'. *Psychology Today*, 29 August 2014 [Online]: https://www.psychologytoday.com/blog/behind-online-behavior/201408/the-psychology-behind-social-media-interactions

MarkMonitor (2013) 'Shopping Report 2012'. [Online]: https://www.markmonitor.com/download/report/MarkMonitor_Shopping_Report-2012.pdf

MarkMonitor (2015) 'Resources to stop counterfeiters'. [Online]:

https://www.markmonitor.com/resources/stop_counterfeiters.php

Mark Monitor (2015) 'Resources'. [Online]: https://www.markmonitor.com/resources/

MarkMonitor (2015) 'Global Consumer Shopping Habits Survey'. [Online]: https://www.markmonitor.com/download/report/MarkMonitor_Online_Barometer-2015.pdf

MarkMonitor (2016) 'How Fashion and Luxury Brands are Turning the Tide Against Rogue Websites'. [Online]: https://www.markmonitor.com/download/wp/Markmonitor_Fashion_Luxury_WhitePaper.pdf

Martin, A.J. (2015) 'UK/China cyber security deal: National security attacks still OK, it seems'. *The Register* 22 October 2015 [Online]: www.theregister.co.uk/2015/10/22/uk_china_cyber_security_agreement_ip/

McAllister, N. (2014) 'The EFF blows Snapchat a raspberry in gov't surveillance report'. *The Register* [Online]: http://www.theregister.co.uk/2014/05/15/eff_whos_got_your_back_2014/

McCarthy, K. (2015) 'It's official: Tor's onion domains must be kept off the public Internet'. *The Register,* 28 October 2015. Online]: www.theregister.co.uk/2015/10/28/onion_kept_off_public_internet/

McCracken, H. (2015) 'Inside Mark Zuckerberg's Bold Plan For The Future Of Facebook Behind the Brand'. *The Fast Company*. [Online] http://www.fastcompany.com/3052885/mark-zuckerberg-facebook

McGrory, R. (2015) 'Social Media Statistics for 2015'. *Social Media Ltd* [Online]: http://www.rosemcgrory.co.uk/2015/01/06/uk-social-media-statistics-for-2015/

Meeker, M. (2014) 'Internet Trends 2014 – Code Conference' Kleiner, Perkins, Caufield Byers, San Fransisco, CA [Online] http://kpcbweb2.s3.amazonaws.com/files/85/Internet_Trends_2014_vFINAL_-_05_28_14-_PDF.pdf?1401286773

Mellon, J. and Chalabi, A. (2014) *Fast Forward: The Technologies & Companies Shaping Our Future*. Fruitful Publications, Isle of Man.

Mirani, L. (2015). 'These documents reveal the EU's thoughts on regulating Google, Facebook, and other platforms'. *Quartz* [Online]: http://qz.com/389905/these-documents-reveal-the-eus-thoughts-on-regulating-google-facebook-and-other-platforms/

Morales, A.C. (2005). 'Giving firms an "E" for effort: consumer responses to high-effort firms'. *Journal of Consumer Research*, 2005, 31, pages 806–12.

Morozov, E. (2014) 'Facebook isn't a charity. The poor will pay by surrendering their data'. *The Guardian,* 26 April 2015 [Online]: http://www.theguardian.com/commentisfree/2015/apr/26/facebook-isnt-charity-poor-pay-by-surrending-their-data

Morozov, E. (2015) 'Silicon Valley likes to promise 'digital socialism' – but it is selling a fairytale'. *The Guardian,* 1 March 2015 [Online]: http://www.theguardian.com/commentisfree/2015/mar/01/silicon-valley-promises-digital-socialism-but-is-selling-a-fairy-tale

Morozov, E. (2014) 'When Wall Street and Silicon Valley come together – a cautionary tale'. *The Guardian* 25 October 2014 [Online]: http://www.theguardian.com/commentisfree/2014/oct/25/darker-side-pay-per-laugh-innovations-silicon-valley

Morozov, E. (2015) 'Where Uber and Amazon rule: welcome to the world of the platform'. *The Guardian,* 7 June 2015 [Online]: http://www.theguardian.com/technology/2015/jun/07/facebook-uber-amazon-platform-economy

Morozov, E. (2016) 'The celebrity privacy case that exposes hypocrisy of Silicon Valley power brokers'. *The Guardian,* 28 May 2016 [Online]: http://www.theguardian.com/media/2016/may/28/gawker-hulk-hogan-silicon-valley-privacy-peter-thiel

Murgia, M. (2015) 'Islamic State's detailed security manual reveals its cyber strategy'. *Telegraph* 20 November 2015 Online]: http://www.telegraph.co.uk/technology/internet-security/12007170/I...ic-States-detailed-security-manual-reveals-its-cyber-strategy.html

MusicAlly (2016) 'European Union report tries to quantify music piracy', 25 May 2016 [Online]: http://musically.com/2016/05/25/european-union-report-tries-to-quantify-music-piracy/

Music & Copyright Newsletter (2015) 'Music piracy: No longer headline news, but the problem persists with big brand support'. 5 August 2015 [Online] https://www.ovum.com/research/music-piracy-no-longer-headline-news-but-the-problem-persists-with-big-brand-support/

Naim, M. (2005) *Illicit: how smugglers, traffickers and copycats are hijacking the global economy*. IDB Cultural Centre, Anchor/Random Books, New York, NY

National Trading Standards Board (2014) 'Summary of Activities April 2013 to March 2014'. Pages 18–20 [Online]: http://www.wlga.gov.uk/regulatory-services-publications/national-trading-standards-board-summary-of-activities-april-2013-to-march-2014

Needleman, S.E. (2009) 'For Companies, a Tweet in Time Can Avert PR Mess'. *Wall Street Journal* [Online]: http://www.wsj.com/articles/SB124925830240300343

NetNames (2015) 'Counting the Cost of Counterfeiting: A NetNames Report' [Online]: https://www.netnames.com/assets/shared/whitepaper/pdf/NetNames-Counterfeiting-Report-A4-2015.pdf

OECD (2008) *The Economic Impact of Counterfeiting and Piracy*. OECD, Paris [Online]: http://www.oecd-ilibrary.org/trade/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en

OECD (2009) 'Magnitude of counterfeiting and piracy of tangible products: An Update', November 2009 [Online]: http://www.oecd.org/sti/ind/44088872.pdf

OECD (2015) 'Enquiries Into Intellectual Property's Economic Impact' [Online]: http://www.oecd.org/sti/ieconomy/KBC2-IP.Final.pdf

OECD and EUIPO (2016) *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*. OECD Publishing, Paris.

Ofcom (2013) 'Adult Media Literacy' [Online]: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf

Ofcom (2014) 'Adult Media Literacy' [Online]: https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults-media-use-and-attitudes

OHIM (2013) 'Impact of intellectual property rights intensive industries in the European Union' [Online]: https://oami.europa.eu/ohimportal/en/web/observatory/ip-contribution

OHIM (2013) 'European Citizens and Intellectual Property: Perception, Awareness and Behaviour' [Online]: https://euipo.europa.eu/ohimportal/documents/11370/80606/IP+perception+study

OHIM (2015) 'The Economic Cost of IPR Infringement in the Clothing, Footwear and Accessories Sector' [Online]: https://oami.europa.eu/ohimportal/en/web/observatory/ip-infringements_clothing-accessories-footwear

OHIM (2015) 'The economic cost of IPR infringement in the cosmetics sector' [Online]: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/quantification-of-infringement-cosmetics_en.pdf

OHIM, (2015). 'Economic Studies in the Observatory – Conference on Policy and Stakeholder Perspectives to Prevent Counterfeiting and Illicit Trade, Brussels'. 16 June 2015. [Online] http://www.coalitionagainstillicittrade.org/wp-content/uploads/2015/07/OHIM_Obs-economic-studies-CEPs-June-2016_Patrice-Pellegrino.pdf

OHIM/Europol (2015) 'Situation Report on Counterfeiting in the European Union' [Online]: https://euipo.europa.eu/ohimportal/documents/11370/80606/2015+Situation+Report+on+Counterfeiting+in+the+EU

Our Social Times (2015) 'Useful Social Media Statistics for 2015' [Online]: http://oursocialtimes.com/8-useful-social-media-statistics-for-2015/

Orlowski, A. (2015) 'Google-chaired think tank says Google's No.1 for digital rights'. *The Register* [Online]: www.theregister.co.uk/2015/11/06/new_america_foundation_praises_google/

Page, L. (2015) 'Google Investor Relations: Google Announces Plans for New Operating Structure'. 10 August 2015 [Online]: https://abc.xyz/investor/founders-letters/2015/

Perrin, A. (2015) 'Social Media Usage: 2005–2015'. *Pew Research Center* [Online]: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

Phillips, T. (2005) *Knockoff: The Deadly Trade in Counterfeit Goods*. Kogan Page Ltd., London and Sterling VA

Poddar, A., Foreman, J., Banerjee, S. and Scholder, E.P. (2011) 'Exploring the Robin Hood effect: Moral profiteering motives for purchasing counterfeit products'. *Journal of Business Research*, Volume 65, Issue 10, October 2012, pages 1,500–1,506, JBR-07390 Elsevier.

Prabhakar, H. (2012) *Black Market Billions: How organised retail crime funds global terrorists*. FT Press/Pearson Education Limited, New Jersey

Press Association (2015) 'Rats' droppings, human urine and arsenic... Police warn against counterfeit cosmetics'. *The Guardian*, 18 May 2015 [Online]: http://www.theguardian.com/fashion/2015/may/18/police-campaign-dangers-counterfeit-cosmetics

Price, E. (2015) 'Sean Parker on tech industry's "tricks": Social media feeds our narcissism'. *The Guardian*, 9 November 2015 [Online]: http://www.theguardian.com/technology/2015/nov/09/sean-parker-social-media-facebook

Quinn, B., Ball, J. and Rushe, D. (2014) 'GCHQ chief accuses US tech giants of becoming terrorists' "networks of choice"'. *The Guardian*, 3 November 2014 [Online]: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan

Rand Corporation (2012) 'Measuring IPR infringements in the internal market – Development of a new approach to estimating the impact of infringements on sales' [Online]: Measuring+IPR+infringements+in+the+internal+market +Develop-ment+of+a+new+approach +to+estimating+the+impact+of+infringements+on+sales

Recode (2015) 'Twitter planning company-wide lay-offs', 9 October 2015 [Online]: http://recode.net/2015/10/09/twitter-is-planning-company-wide-layoffs-for-next-week/

The Register (2015) 'Google officially doubles EU lobbying – but true figure is surely higher', 29 April 2015 [Online]: www.theregister.co.uk/2015/04/29/google_doubles_eu_lobbying/

Rifkin, J. (2014) *The Zero Marginal Cost Society*. Palgrave Macmillan, New York.

Roberts, A. (2015) 'Luxury Firms Fight Online Fraudsters Over Expensive Fakes'. *Bloomberg*, 27 July 2015 [Online]: http://www.bloomberg.com/news/articles/2015-07-27/fakes-at-7-800-send-luxury-companies-online-to-fight-fraudsters

Schatten, M., Seva, J. and Okresa-Duric, B. (2015) 'Big Data Analytics and the Social Web: A Tutorial for the Social Scientist'. *European Quarterly of Political Attitudes and Mentalities* (EQPAM), Volume 4, No 3, July 2015.

Schindler, J. (2015) 'New anti-counterfeiting union announced as regulator blasts Alibaba over fakes'. *Blog – World Trademark Review* [Online]: http://www.worldtrademarkreview.com/Blog/detail.aspx?g=79b06ebf-203a-4ed4-8992-6a2c6d66affa

Seetharaman, D. (2015) 'Facebook Prods Users to Share a Bit More'. *Wall Street Journal* [Online]: http://www.wsj.com/articles/facebook-prods-users-to-share-a-bit-more-1446520723

Seetharaman, D. (2015) 'Fake Accounts Still Plague Instagram Despite Purge, Study Finds'. *Wall Street Journal*, 30 June 2015 [Online]: http://blogs.wsj.com/digits/2015/06/30/fake-accounts-still-plague-instagram-despite-purge-study-finds/

Severin, K. (2016) 'MIDIA Research' [Online]: https://www.midiaresearch.com/blog/facebooks-deeptext-sees-and-learns-from-everything-you-write/ https://code.facebook.com/posts/181565595577955/introducing- deeptext-facebook-s-text-understanding-engine/

Sky News (2015) 'Instagram overtakes Twitter with 400m users' [Online]: http://news.sky.com/story/1557462/instagram-overtakes-twitter-with-400m-users

Smith, K. (2016) 'Marketing: 96 Amazing Social Media Statistics and Facts for 2016'. *Brandwatch* [Online]: https://www.brandwatch.com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016/

Solon, O. (2016) 'How Facebook plans to take over the world'. *The Guardian*, 23 April 2016 [Online]: https://www.theguardian.com/technology/2016/apr/23/facebook-global-takeover-f8-conference-messenger-chatbots

Sparkes, M. (2014) 'Instagram Users this year overtook Twitter in terms of global users'. *The Telegraph* [Online]: http://www.telegraph.co.uk/technology/facebook/11285727/Instagram-overtakesTwitter-to-reach-300m-users.html

Speechlys LLP (2015) 'Will Facebook face-off the Belgium Courts?' *Lexology*, 23 November 2015 [Online]: http://www.lexology.com/library/detail.aspx?g=ef8086a4-6b00-462a-8741-bee89562047b

Spink, J. and Fejes, Z.L. (2012) 'A review of the economic impact of counterfeiting and piracy methodologies and assessment of currently utilized estimates'. *International Journal of Comparative and Applied Criminal Justice*, Volume 36, Issue 4, 2012.

Stroppa, A., di Stefano, D. and Parrella, B. (2016) 'Social media and luxury goods counterfeit: a growing concern for government, industry and consumers worldwide' [Online]: https://www.washingtonpost.com/blogs/the-switch/files/2016/05/IG_A2016_ST2.pdf?tid=a_inl

Stumpf, S.A. and Chaudhry, P.E. (2010) 'Country matters: Executives weigh in on the causes and counter measures of counterfeit trade'. *Business Horizons*. http://www.peggychaudhry.com/publications/business-horizons-matters.pdf

Stumpf, S.A., Chaudhry, P.E. and Perretta, L. (2011) 'Fake: can business staunch the flow of counterfeit products?'. *Journal of Business Strategy*, March 2011, Volume 32, Issue 2.

Sundberg, J. (2015) 'How to Rank Better on Google: SEO Tips'. Undercover Recruiter [Online]: http://theundercoverrecruiter.com/infographic-how-you-can-rank-better-on-google-seo-tips/

Thaler, R. (2015) *Misbehaving: The making of behavioural economics*. Penguin Books Limited (UK), 2016

Tiku, N. (2016) 'Facebook Wants To Be The Layer Between You And The Future'. *Buzzfeed News*, 13 April 2016 [Online]: https://www.buzzfeed.com/nitashatiku/facebook-wants-to-be-the-layer-between-you-and-the-future

Titcomb, J. (2015) 'Facebook "snooping" requests increase 60 per cent in UK'. *Telegraph*, 11 November 2015 [Online]: http://www.telegraph.co.uk/technology/facebook/11989781/Facebook-snooping-requests-increase-60-per-cent-in-UK.html

Torrentfreak (2015) 'Google Asked to Remove 1,500 "Pirate Links" Per Minute' [Online]: https://torrentfreak.com/google-asked-to-remove-1500-pirate-links-per-minute-151122/

Torrentfreak (2015) 'Google opposes whole-site removal of "pirate" domains' [Online]: https://torrentfreak.com/google-opposes-whole-site-removal-of-pirate-domains-151021/

Torrentfreak (2015) 'Google Asked to Remove One Billion "Pirate" Search Results' [Online]: https://torrentfreak.com/google-asked-to-remove-one-billion-pirate-search-results

Torrentfreak (2016) 'UK Government expands crackdown on online piracy' [Online]: https://torrentfreak.com/uk-government-expands-crackdown-on-online-piracy-160510/

Travis, A. (2015) 'May calls for Internet companies to store details of website visits'. *The Guardian*, 3 November 2015 [Online]: http://www.theguardian.com/politics/2015/nov/03/may-calls-for-internet-companies-to-store-details-of-website-visits

Tumblr (2015) 'Terms of Service' [Online]: https://www.tumblr.com/policy/en/terms-of-service

Turner, K. (2016) 'That Chanel bag on your Instagram feed may not be a Chanel bag'. *The Washington Post*, 26 May 2016 [Online]: https://www.washingtonpost.com/news/the-switch/wp/2016/05/26/that-chanel-bag-on-your-instagram-feed-may-not-be-a-chanel-bag/

Twitter (2015) 'Trademark Transparency Report'. June 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jan-jun

Twitter (2016) 'Trademark Transparency Report'. December 2015 [Online]: https://transparency.twitter.com/trademark-notices/2015/jul-dec

UK Government (2000) 'Regulation of Investigatory Powers Act 2000' [Online]: http://www.legislation.gov.uk/ukpga/2000/23/section/49

UK Government (2015) 'Home Secretary oral statement to Parliament on publication of the Anderson report' [Online]: https://www.gov.uk/government/speeches/home-secretary-on-publication-of-the-anderson-report

UK Government (2015) 'The use of social media for online radicalization' [Online]: https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

UK Government (2016) 'Press notice: "Take economic statistics back to the future," says Charlie Bean' [Online]: https://www.gov.uk/government/publications/independent-review-of-uk-economic-statistics-final-report/press-notice-take-economic-statistics-back-to-the-future-says-charlie-bean

United Nations Office on Drugs and Crime (UNODOC) 'Focus on the Illicit Trafficking of Counterfeit Goods and Transnational Organised Crime' [Online]: http://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf

Urban, J.M., Karaganis, J. and Schofield, B.L. (2016) 'Notice and Takedown in Everyday Practice'. UC Berkeley, Public Law Research Paper No 2755628. *SSRN* [Online]: http://ssrn.com/abstract=2755628

U.S. Department of Homeland Security (2014) 'Intellectual Property Rights Seizures Statistics'. Fiscal year 2014 [Online]: https://www.cbp.gov/sites/default/files/documents/IPR%20FY14%20Seizure%20Statistics%20Booklet_100515_spread_web.pdf

U.S. General Accounting Office/GAO (2010) 'Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods' [Online]: http://www.gao.gov/products/GAO-10-423

US ITC (2010) 'China's Systemic Counterfeiting and IP Theft Undermine U.S. Economic and National Security | The Innovation Files – A broad report by the U.S. International Trade Commission (ITC) on Chinese Intellectual Property Infringement' [Online]: http://www.innovationfiles.org/chinas-systemic-counterfeiting-and-ip-theft-undermine-u-s-economic-and-national-security/

U.S. Securities and Exchange Commission (2016) https://www.sec.gov/edgar.shtml

Vax, M. (2015) 'The Internet is about to take a U-turn – is your business prepared?' *The Future of Commerce,* 18 May 2015 [Online]: http://www.the-future-of-commerce.com/2015/05/18/the-internet-is-about-to-go-from-pull-to-push-is-your-business-prepared/

VDMA (2014) 'Product Piracy' [Online]:http://pks.vdma.org/article/-/articleview/3842960

The Verge (2015) 'Facebook is unleashing universal search across its entire social network' 22 October 2015. Online]: http://www.theverge.com/2015/10/22/9587122/new-facebook-search-all-public-posts

Von Lohmann, F. (2015) 'A Step Toward Protecting Fair Use on YouTube'. *Google Public Policy Blog*, 19 November 2015 [Online]: http://googlepublicpolicy.blogspot.co.uk/2015/11/a-step-toward-protecting-fair-use-on.html

Which? (2015) 'How to spot a fake or fraudulent or scam website' [Online]: http://www.which.co.uk/consumer-rights/advice/how-to-spot-a-fake-fraudulent-or-scam-website

Wilson, J. and Sullivan, B. (2016) 'Brand owner approaches to assessing the risk of product counterfeiting'. *Journal of Brand Management*, May 2016, Volume 23, Issue 3, pages 327–344.

Wilson, J., Sullivan, B. and Hollis, M. (2016) 'Measuring the "Unmeasurable": Approaches to Assessing the Nature and Extent of Product Counterfeiting'. *International Criminal Justice Review*. 1057567716644766.

World Customs Organization (2015) 'IPM – The WCO tool in the fight against counterfeiting' [Online]: http://www.wcoipm.org/__resources/userfiles/file/IPM-Brochure.pdf

World Trademark Review (2015) 'Supply and demand: the need for a comprehensive approach to combating' [Online]: http://www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2015/Introduction/Supply-and-demand-the-need-for-a-comprehensive-approach-to-combating

World Trademark Review (2015) 'Global strategies for protecting brands in the expanded online space' [Online]: http://www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2015/Industry-insight/Global-strategies-for-protecting-brands-in-the-expanded-online-space

World Trademark Review (2015) 'Cooperation to combat counterfeiting' [Online]: http://www.worldtrademarkreview.com/Intelligence/Anti- counterfeiting/2015/Introduction/Cooperation-to-combat-counterfeiting

http://www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2015/Introduction/Cooperation-to-combat-counterfeiting

World Trade Organisation (2016) 'World Trade Organisation's Trade Related Aspects of Intellectual Property Rights' [Online]: https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm

Videos

BBC (2013) Fake Britain [Online]: https://www.youtube.com/watch?v=-ezrVVtx9uU (16 May 2013)

Canadian Broadcast Company (2011) *Counterfeit Culture* [Online]: http://www.cbc.ca/doczone/episodes/counterfeit-culture

Counterfeit Culture [Online]: https://www.facebook.com/CounterfeitCultureHornby, N./Blast Films (2008) *Fake Trade* [Online]: http://topdocumentaryfilms.com/fake-trade/ https://www.youtube.com/watch?v=tVXubFu7GZM (6 September 2014)

http://topdocumentaryfilms.com/fake-trade/#comments

Foerster, M. (2015) *Made in China – Factory of the World*, 6 May 2015 Discovery Channel [Online]: https://www.youtube.com/watch?v=fDS8co75xFc

Concept House
Cardiff Road
Newport
NP10 8QQ

Tel: 0300 300 2000
Fax: 01633 817 777

For copies in alternative formats please contact our Information Centre.

When you no longer need this booklet, please recycle it.

DPS/ERE/07/17

INVESTORS IN PEOPLE

CUSTOMER SERVICE EXCELLENCE