Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR

Natalija Vlajic
EECS Department
Lassonde School of Engineering
York University
Toronto Canada
vlajic@cse.yorku.ca

Marmara El Masri
EECS Department
Lassonde School of Engineering
York University
Toronto Canada
marmara@my.yorku.ca

Gianluigi M. Riva
School of Information and Communication Studies
University College Dublin
Dublin Ireland
gianluigi.riva@ucd.ie

Marguerite Barry
School of Information and Communication Studies
University College Dublin
Dublin Ireland
marguerite.barry@ucd.ie

Derek Doran
Dept. of Computer Science & Engineering
Wright State University
Dayton OH USA
derek.doran@wright.edu

ABSTRACT

The recent news of a large-scale online tracking campaign involving Facebook users, which gave way to systematic misuse of the collected user-related data, has left millions of people deeply concerned about the state of their online privacy as well as the state of the overall information security in the cyber world. While most to-date revelations pertaining to user tracking are related to websites and social media generally intended for adult online users, relatively little is known about the prevalence of online tracking in websites geared towards children and teens.

In this paper, we first provide a brief overview of two laws that seek to protect the privacy of kids and teens online – the US Children’s Online Privacy Act (COPPA) and the EU General Data Protection Regulation (GDPR). Subsequently, we present the results of our study which has looked for potential signs of user tracking in twenty select children-oriented websites in case of a user located in the USA (where COPPA is applicable) as well as a user located in the EU (where GDPR is applicable). The key findings of this study are alarming as they point to overwhelming evidence of widespread and highly covert user tracking in a range of different children-oriented websites. The majority of the discovered tracking is in direct conflict with both COPPA and GDPR, since it is performed without parental consent and by third-party advertising and tracking companies. The results also imply that, relative to their US counterparts, the children residing in the EU may be somewhat less subjected (but are still significantly exposed) to tracking by third-party companies.

KEYWORDS

User privacy; online tracking; COPPA; GDPR

ACM Reference format:
Natalija Vlajic, Marmara El Masri, Gianluigi M. Riva, Marguerite Barry and Derek Doran. 2018. Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. In 2nd Int’l Workshop on Multimedia Privacy and Security (MPS ’18), Oct. 15, 2018, Toronto, ON, Canada, 8 pages. https://doi.org/10.1145/3267357.3267370

1 ONLINE TRACKING: PROS, CONS, COPPA and GDPR

1.1 Pros and Cons of Online Tracking

The term online tracking refers to the process of recording, measuring, and analyzing the behavior of individual human users while browsing the WWW. On one hand, from the financial performance perspective, this process is seen as one of the key drivers for optimization and growth of online-based businesses and organizations (namely, understanding how customers behave and what they want has always been the key to success of any business in any industry). On the other hand, from the perspective of individual users, online tracking is considered to be a major threat to online privacy, as it can lead to extraction and leakage of sensitive personal information. Furthermore, the recent incidents involving the tracking of Facebook users, which gave way to unscrupulous misuse of the collected data by third parties (Cambridge Analytica, in particular), have shown that the negative implications of online tracking can now easily cross the boundaries of the cyber-domain and impact the operation and stability of the actual real world [1].
Ultimately, users of all ages (adults and children) can be subjected to online tracking for a range of different reasons (e.g., commercial, financial, political, national security, etc.). However, when it comes to online tracking of children, one single motivator/driver stands out, and that is 'commercial advertising'. As pointed out in [2], children represent critically important demographics to marketers because: 1) they have considerable influence on their parents' buying decisions, 2) they, themselves, own significant purchasing power, and 3) they are the adult consumers of the future. In terms of numbers, according to [3], the children’s digital AD market has been experiencing an astonishing 25% year on year growth, and is expected to reach US $1.2 billion by 2019.

In order to effectively market to children, modern-day digital advertising companies: a) rely on teams of well-paid researchers and psychologists, b) take advantage of a wealth of in-depth studies about children’s development, emotional and social needs at different ages [2], and c) make use of an abundance of personalized data largely obtained by means of online tracking. And, that is where the heart of the problem pertaining to digital advertising and online tracking of children lies, as numerous research works have shown that children (and even young adolescents) “lack the cognitive skills to understand the persuasive intent of the skillfully crafted and highly targeted online advertising” [4]. In other words, modern-day digital/online advertising can be harmful to mental and psychological development of children, in addition to potentially causing considerable financial as well as other types of stresses to their respective families.

### 1.2 COPPA

The Children’s Online Privacy Protection Act (COPPA) is a US federal law that was first enacted in October 1998 [5] and then subsequently amended in January 2013 [6]. The COPPA legislation was put in place to regulate (i.e. limit) the collection, use or disclosure of personal identifiable information (PII) of children and youth by the following two categories of operators: A) operators of commercial websites and online services, including mobile apps, directed to children under the age of thirteen, as well as B) operators of general-audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under the age of thirteen. (In COPPA, PII refers to a range of different personal information identifiers, including: full name; home/physical address; online contact information, like an email address; telephone number; social security number; ‘persistent Internet identifier’, including cookie number, an IP address, a unique device identifier like a MAC address, etc.)

Now, the sites/services that are directed to children and are unmistakably covered by COPPA (i.e., category A operators) are strictly prohibited from collecting any PII until they:

A.1) Give a direct notice to the child’s parent about its information practices, which should: i) explain which specific PII the site/service is set to collect and how this information might be disclosed to others; ii) enlist all third-party operators, such as advertising or social networks, that collect children’s PII through this site/service; iii) provide a clear description of all parental rights over their child’s collected PII.

A.2) Obtain the parent’s verifiable consent to collect their child’s PII. (Various methods can be used to confirm the parent’s identity, including: receive a signed and mailed consent form, accept and verify the parent’s credit card number, receive an email with the parent’s valid digital signature, etc.)

The operators of general-audience sites/services that do not target children as their primary audience but are directed to children based on other factors [7] (i.e., category B operators) are specifically required to refrain from collecting PII from any visitor to their site/service before verifying the visitor’s age. If the visitor turns out to be a child under the age of 13, the site/service has two options:

B.1) Offer the visitor different activities and functions than those that are offered to adult visitors and that include collection of users’ PII.

B.2) Proceed in the same manner as operators of category A (i.e., request the parent’s verifiable consent prior to engaging in any collection of the visitor’s PII).

It is important to note that a site/service that does not collect PII from children directly, but instead enables another (third-party) company to do so through their site/service, is also required to comply with COPPA. Moreover, in such a case, the third-party company must adhere to COPPA as well, if it has actual knowledge that it is collecting personal information from a child-directed site/service [7].

However, it should also be pointed out that, according to COPPA, in certain circumstances a site/service (including a third-party site/service) may be allowed to collect children’s PII without parental consent, (e.g.) provided the collected PII is explicitly used to support one or more of the site’s/service’s ‘internal operations’, such as: a) authenticate users; b) protect user or site security; c) ensure regulatory compliance, d) generate personalized content; e) serve contextual advertising, etc. [7]. It should be noted here that contextual advertising refers to ads that are delivered based on one single visit/use of a given site/service and without regards for the user’s behavior or previous interactions with this or other sites/services [8]. On the other hand, behavioral advertising - which is strictly prohibited by COPPA! - aims to deliver highly targeted ads to each individual user based on the profile that is built by tracking this user’s behavior over longer period of time and across various sites and services. Unfortunately, as pointed out in [8], determining whether the PII collected by a first- or third-party site/service is being used to serve contextual vs. behavioral advertising is very hard if not impossible, as that would require in-depth knowledge of the internal business practices of the company owning the given site/service.

Unfortunately, ever since COPPA was passed, the on-the-ground implementation of this legislation was slow and problematic, with sporadically reported incidents of websites and services either avoiding or violating many of COPPA provisions [9]. In the most recent of such incidents, the Disney
company (often considered to be the ‘gold standard’ when it comes to ‘customer experience’ and ‘user trust’) has been alleged of violating COPPA in 42 of their online apps [10]. The second more recent case (April, 2018) involves YouTube (now owned by Google), which is used by 80% of American children ages 6 to 12. According to [11], 20 child advocacy, consumer and privacy groups have filed a complaint with the FTC claiming that YouTube is violating COPPA by: 1) having the actual knowledge that children under 13 constitute a significant percentage of their users, and 2) not implementing any measures to identify such users, limit their tracking or obtain verifiable parental consent for their tracking. If the FTC finds that YouTube has violated COPPA, they may be forced to impose an ‘age gate’ on their users, which will be an important precedent for other similar services and tech giants [11].

1.3 GDPR

On the 25th of May 2018, the General Data Protection Regulation (GDPR) [12] came into effect in the 28 member countries of the European Union (EU). It represents a new EU landmark in the protection of users’ personal data (PD) and privacy. It should be pointed here that unlike the USA, the EU does not have a separate law pertaining to the protection of children’s data and privacy, but instead addresses this issue through several general provisions stated in the GDPR. (The sections of the GDPR that relate to children’s data and privacy are referred to by the acronym GDPR-K.) Namely, the GDPR is written with a wider focus than COPPA and aims to provide a flexible legal framework that can be further customized by individual EU member states. Nevertheless, the GDPR’s provisions are (still) sufficient to support a legal regime that is as strong as COPPA when it comes to the protection of children’s privacy online.

In its essence, the GDPR is intended to regulate the “processing of personal data wholly or partly by automated means...” [13] and “the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not” [14]. It also applies “to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union...” [15]. GDPR Article 8 specifically addresses the concept of ‘minors’ digital consent’, fixing the age threshold at 16, although the individual EU members can set it to a lower age, limited at 13. Below this age, parental consent for collection of personal information from minors is required, using mechanism similar to those outlined in COPPA.

One of the most significant GDPR-K provisions that, unfortunately, is not covered by COPPA is the so called ‘right to erasure’, also known as ‘right to be forgotten’. In particular, according to Article 17 of GDPR, even in cases when personal data about children have been collected on the basis of consent, individuals have the right to erasure of their data. The article is particularly relevant in cases where the data subject has given his/her consent as a child not fully aware of the risks involved by the process, and later wants to remove such data. The right to erasure is exercisable notwithstanding the fact that the data subject may no longer be a child.

2 ONLINE TRACKING: TECHNIQUES & IMPLEMENTATIONS

2.1 Online Tracking Techniques

According to [9], the most common techniques of online user tracking, together with their most significant pros and cons, include:

- **IP based tracking** allows tracking of users on multiple websites belonging to different entities and cannot be prevented by simple change(s) in browser settings. However, this form of tracking does not work very well in several (increasingly common) situations, such as: the user owns/uses one or more mobile devices, the user deploys IP-anonymization, multiple users share the same computer.

- **Cookie based tracking** requires that a small piece of server-generated data first be explicitly stored on the user’s device upon his initial visit to a website/server, and then this piece of data is returned to the given server whenever the user revisits the same/ respective website. While generally very effective and, as a result, the most widely deployed form of user tracking in practice, cookie based tracking can be obstructed if the user disallows or cleans cookies from his browser. (Based on the statistics provided by [16], cookies are deployed by nearly 50% of all WWW sites.)

- **Cache (i.e., Etag) based tracking** avoids storing explicit tracking data in the client’s memory, but instead relies on server-generated data/objects that get implicitly and automatically stored in the browser’s cache (such as Etags which get exchanged by means of HTTP headers). This form of tracking can also be obstructed if the user regularly clears his browser cache. (According to [16], Etags are used only by 14.2% of all websites.)

- **Session based tracking** does not require that any server-generated data get stored in the browser’s memory or cache. Instead, the server inserts user/session-id into all relevant URLs sent to the user. Unfortunately, the main drawback of session based tracking is that it is very ‘visible’ and cannot be easily obscured from the user, unlike the other three methods.

Given that all of the above described tracking techniques (including the most popular and prevalent of them - cookie based tracking) come with their own set of drawbacks, most real-world websites combine two or more of these techniques.

2.2 Online Tracking Implementations

An actual ‘data exchange’ between a tracking company and a tracked user is the key precondition for either of the above enlisted tracking techniques to be utilized in practice. In other words, a tracking company is able to start tracking a user only after the user’s browser has been engaged in an HTTP request/response exchange with one of the company’s content servers. Clearly, if the tracking company is the owner of a
website knowingly visited by the user (a first-party tracker) tracking is rather trivial to implement, as numerous HTTP exchanges will automatically take place between the user’s browser and the company’s content server(s). On the other hand, for companies that do not necessarily own Web content but are rather in the business of collecting user-related data (third-party trackers) tracking is somewhat more challenging to carry out. Namely, a third-party tracker requires that either a ‘tracking pixel’ (a small invisible image) or a ‘tracking snippet’ (typically small pieces of JavaScript code) be hosted/hidden in the webpages of actual Web content provider(s) in order to trigger/solicit the required data exchange between the user’s browser and the third-party tracking server(s). For an illustration, see Figure 1.

Figure 1: Tracking snippet as a facilitator of user tracking by third-party trackers

It should be pointed here that (hidden) tracking snippets are particularly advantageous form/facilitators of user tracking, both for first-party and third-party trackers. This is because a piece of JavaScript code can not only serve to initiate a data exchange with a tracking server (thus enabling the utilization of either of the four tracking mechanisms), but it can also enable the tracking server to monitor the user actions during his/her viewing of the given page (i.e., gather information on how long the user stayed on the page, which button he/she clicked, etc.), as well as to obtain information about the capabilities of the user’s browser. According to [16], 65.5% of websites contain some form of JavaScript-based tracking snippets. Also, many of the real-world tracking snippets initiate the retrieval of small invisible images as a means of facilitating data exchange with multiple third-party tracking servers.

3 EXPERIMENTAL OBJECTIVES

Our analysis of the twenty selected websites was conducted using Chrome’s Developer Tools and custom-made Python scripts. Copies of the analyzed pages were retrieved by several different web clients (i.e., computers) holding a U.S. IP address (May 23rd – May 30th, 2018) and a U.E. address (June 14th – June 17th, 2018). The webpages and HTTP response and request headers for the images were largely manually analyzed, and the Python scripts served to help automate more nuanced aspects of the data collection, such as converting HAR files that contained the webpages to CSV files that were easier to analyze and such.

The main objectives of our research were twofold:

- Study several representative websites found in Alexa’s top 50 ‘Kids and Teens’ category as well as some allegedly COPPA-compliant websites for potential signs of user tracking. In particular, we have concentrated our attention to websites from four specific categories: general/education sites (from Alexa top 50), gaming sites (from Alexa top 50), allegedly COPPA-compliant sites (have COPPA compliant stamp and policy on website), and child-related NPO sites, as enlisted in Table 1.
- Specifically focus on finding the signs of user tracking by means of (invisible) images embedded/placed in the websites enlisted above. Namely, from the perspective of online user tracking, images represent ‘perfect Trojans’ since: (a) today’s users are accustomed to retrieving/viewing webpages that are graphically very rich (i.e. contain a large number of embedded images often hosted at different web domains), (b) during the rendering of a requested webpage, all of its embedded images (regardless of their actual number, size or their respective domains of origin) are automatically and instantaneously retrieved by all commercial browsers operating in their default settings, (c) most web vulnerability scanning tools perform minimal if any scanning of images for potential signs of misuse, and (d) in order to prevent retrieval and displaying of images, a user would have to be sufficiently skilled and knowledgeable on how to appropriately modify the default settings of his browser.

4 EXPERIMENTAL RESULTS

The most important findings of our study are presented in Tables 2 to 7 and in Figures 2 and 3. In particular:

- Tables 2 and 3 give an overview of the percentage of images (found in each of the twenty examined sites) based on their domain of origin, which can be: a) a server owned by an advertising or advertising delivery company, b) the server hosting the actual examined website/webpage, c) a server owned by a Web analytics company, and d) a server owned by a Web tracking company. The numbers in Table 2 are specifically derived by analyzing the ‘copies’ of the twenty select webpages after they are retrieved from a US IP address (i.e., by a Web user residing in the USA). Table 3, on the other hand, is derived by analyzing the ‘copies’
of the same twenty pages after they are retrieved from an EU IP address (i.e., by a Web user residing in the EU).

- Tables 4 and 5 follow a similar breakdown of images based on their domain of origin, though their purpose is to show which percentage of images in each particular category is ‘invisible’ (i.e., obscured or never shown to the user). As explained in Section 2, the most likely purpose of ‘invisible’ images is user tracking.
- Tables 6 and 7 show the percentages of images in each category that carry cookies.
- Figures 2 and 3 contain histograms showing the total number of examined sites (out of twenty) that contain one or more invisible images hosted by a particular third-party company as recorded for a US and an EU user, respectively.

Finally, to be able to put the above enlisted results in perspective, it should be pointed out that while we were able to identify an accessible online privacy policy on all examined websites, only four of these policies warned about the involvement of the respective site with third-party trackers (notably, these were the privacy policies found on bulbagarden.net, nintendo.com, ea.com, pokemon.com). However, neither of the examined sites implemented any age-verification mechanisms, nor attempted to solicit a verifiable parental consent in relation to (potential) third-party tracking of children on most of these sites.

Some of the key observations that can be drawn from the results shown in Tables 2 to 7 and Figures 2 and 3 include:

1. When looking at the origin of the embedded images, while considering the content category of each examined websites (as show in Table 1), the five sites from general/education category appear most problematic (i.e., most likely to subject their visitors to third-party user tracking), as a significant percentage of their images come from third-party AD servers – both in the case of the US and the EU users (see Table 2 and 3).
2. Tables 4 and 5 as well as Tables 6 and 7 support the suspicion that images coming from AD servers and other third-party sites are (in a very large percentage) used for the purposes of user tracking, as most of these images are, in fact, ‘invisible’ and carry cookies. This observation holds not only in the case of five general/education sites, but in the case of the other fifteen sites as well, and applies equally to the US and the EU user.
3. It should be noted, however, that the overall percentage of third-party images in general/education sites is somewhat smaller for the EU relative to the US user (compare Tables 2 to 3). This, potentially, could be attributed to the recent introduction of GDPR in Europe, which may have put pressure on the operators of these sites to reduce the prevalence of user tracking by third-party companies. (A similar trend can be observed in most other sites, except for leagueoflegends.com and childfund.org.)
4. Probably the biggest surprise and disappointment of this study are the results pertaining to the children charity sites, as in some of these sites the presence of third-party trackers is quite pronounced. (E.g., in the case of the US Web user, around 50% of images appearing in children.org and savethechildren.org are likely used for the purposes of user tracking.)
5. In contrast to the general/education and children charity sites, the gaming and COPPA-compliant sites appear rather ‘clean’ and trustworthy, as majority of their images come from the actual ‘host’ domain (see Tables 2 and 3). The likely explanation for this observation lies in the fact that websites in these two categories, unlike the other ten examined sites, have their own reliable revenue streams (i.e., they sell their own products or services). Put another way, these sites do not have to rely on third-party tracking and/or digital marketing as important sources of revenue.

6. Finally, in terms of more general across-the-board third-party tracking, Figures 2 and 3 reveals a not-so-surprising fact: two tech giants most frequently implicated in large-scale (often unauthorized) tracking of adult online users - Google and Facebook - also stand out as the most prevalent trackers across various children-oriented sites. Specifically, the ‘invisible’ images hosted by these two companies are detected in 15 and 11 of the twenty examined websites for the US user, and 13 and 10 of the twenty examined websites for the EU user, respectively.

5 CONCLUSIONS

In this paper, we have shown that user tracking of kids and teens by third-party companies is still very prevalent despite the existing laws that clearly prohibit such practices. In particular, the results of our study have revealed that: 1) children-oriented general/educational websites are the most likely facilitators of third-party tracking, as these sites tend to rely on third-party advertising as their main source of revenue, and 2) the users/children protected by the GDPR (i.e., the EU residents) appear somewhat better, but still insufficiently, shielded from third-party tracking relative to their US counterparts.

ACKNOWLEDGEMENTS

This research was supported by the Natural Science and Engineering Research Council of Canada (NSERC). G. M. Riva has received funding as part of TEAM (Technology Enabled Mental Health for Young People) from EU Horizon 2020 under MSC grant agreement No. 722561.

REFERENCES

[1] Alexis C. Madrigal. 2017. What Facebook Did to American Democracy. (November 2017). Retrieved July 16, 2018 from https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/
[2] MediaSmarts. How Marketers Target Kids. Retrieved May, 2018 from http://mediasmarts.ca/digital-media-literacy/media-issues/marketing-consumerism/how-marketers-target-kids
[3] PwC. 2017. Kids Digital Advertising Report 2017. September 2017.
[4] Xiaomei Cai and Xiaquan Zhao. 2013. Online advertising on popular children’s websites: Structural features and privacy issues. Computers in Human Behavior 29, 4 (2013), 1510–1518. DOI: http://dx.doi.org/10.1016/j.chb.2013.03.013
[5] Federal Trade Commission. 1998. Children’s Online Privacy Protection Rule (COPPA), October 1998.
[6] Federal Trade Commission. 2013. Children’s Online Privacy Protection Rule (COPPA): Final Amendments to Clarify the Scope of the Rule and Strengthen Its Protections for Children’s Personal Information, January 2013.
Federal Trade Commission. 2017. Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (July 2017). Retrieved July 16, 2018 from https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari, Bar On, Abbas Razaghpaham, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. “Won’t Somebody Think of the Children?” Examining COPPA Compliance at Scale. Proc. Priv. Enhancing Technol. (2018). DOI:https://doi.org/10.1515/popets-2018-0021.

Lauren A. Matecki (2010). Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. Northwestern Journal of Law & Social Policy 5,2(7).

Matthew Humphries. 2017. Lawsuit Claims Disney Is Violating COPPA, Tracking Kids in 42 Apps. (August 2017). Retrieved July 16, 2018 from https://www.pcmag.com/news/355509/lawsuit-claims-disney-is-violating-coppa-tracking-kids-in-4

Jeff Chester. 2018. Advocates Say Google’s YouTube Violates Federal Children’s Privacy Law. (April 2018). Retrieved May 20, 2018 from https://www.democraticmedia.org/article/advocates-say-gogles-youtube-violates-federal-childrens-privacy-law

Council and European Parliament Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (2016) OJ L119/1, (General Data Protection Regulation - GDPR).

[13] GDPR article 2.
[14] GDPR article 3.1.
[15] GDPR article 3.2.
[16] Web Technology Surveys, "Usage of site elements for websites", May 2018. https://w3techs.com/technologies/overview/site_element/all

### Table 2: Percentage of images detected in the given page based on their domain of origin (from US IP address)

| Domain            | % Ads server/delivery | % content site/domain | % web analytics site/domain | % tracking site/domain |
|-------------------|-----------------------|-----------------------|-----------------------------|------------------------|
| thesesun.com      | 5%                    | 22.75%                | 1.27%                       | 10.13%                 |
| reverse.com       | 82.78%                | 82.78%                | 82.78%                      | 82.78%                 |
| bing.com          | 87.02%                | 72.34%                | 6.38%                       | 4.26%                  |
| howstuffworks.com | 7.97%                 | 13.33%                | 2.67%                       | 9.23%                  |
| citationsmachine.net | 78.57%             | 7.14%                 | 10.71%                      | 0%                     |
| bizzare.com       | 0%                    | 98.92%                | 1.08%                       | 0%                     |
| ignesoflegenda.com | 18.75%               | 71.88%                | 3.13%                       | 6.25%                  |
| bulbagarden.com   | 0%                    | 99.77%                | 0%                          | 0%                     |
| nintendo.com      | 0%                    | 99.92%                | 0%                          | 0.88%                  |
| en.com            | 7.69%                 | 61.54%                | 7.09%                       | 15.38%                 |
| americangogo.com  | 0%                    | 90.77%                | 3.08%                       | 6.15%                  |
| nudgbr            | 0%                    | 93.65%                | 0%                          | 0%                     |
| pokemons.com      | 0%                    | 93.94%                | 3.03%                       | 3.03%                  |
| clibpengue.com    | 0%                    | 79.47%                | 0%                          | 23.01%                 |
| forget.com        | 14.81%                | 66.67%                | 11.11%                      | 7.41%                  |
| children.org      | 18.75%                | 90.18%                | 18.75%                      | 16.36%                 |
| askedtechnews.org | 25%                   | 48.68%                | 2.63%                       | 23.68%                 |
| children.org      | 0%                    | 50%                   | 0%                          | 0%                     |
| childefund.org    | 0%                    | 71.9%                 | 3.13%                       | 12.5%                  |
| childrensfund.org | 6.67%                 | 73.33%                | 0%                          | 0%                     |

### Table 3: Percentage of images detected in the given page based on their domain of origin (from EU IP address)
Table 4: Percentage of detected images that are invisible based on domain of origin (from US IP address)

| Domain               | % AEs server/delivery | % content site/domain | % web analytics site/domain | % tracking site/domain |
|----------------------|------------------------|-----------------------|----------------------------|------------------------|
| thearsusa.com        | 96.15                  | 0                     | 100                        | 87.5                   |
| reverseimage.net     | 97.37                  | 0                     | 100                        | 93.75                  |
| britains.com         | 87.5                   | 2.94                  | 100                        | 100                    |
| howstuffworks.com    | 96.07                  | 10                    | 100                        | 85.71                  |
| citationmachine.net  | 93.94                  | 16.67                 | 100                        | N/A                    |
| bintendo.com         | N/A                    | 0                     | 100                        | N/A                    |
| legianflagends.com   | 100                    | 0                     | 100                        | 100                    |
| bulbagarden.net      | N/A                    | 0                     | 100                        | 100                    |
| nintendo.com         | N/A                    | 0.89                  | N/A                        | 100                    |
| es.com               | 100                    | 0                     | 100                        | 100                    |
| amextravel.com       | N/A                    | 6.78                  | 100                        | 100                    |
| nudg.com             | N/A                    | 0                     | N/A                        | 100                    |
| pokemons.com         | N/A                    | 0                     | 100                        | N/A                    |
| chapelorgan.com      | N/A                    | 0                     | N/A                        | 100                    |
| foopets.com          | 100                    | 0                     | 100                        | 100                    |
| children.org         | 100                    | 0                     | 100                        | 100                    |
| savechildren.org     | 100                    | 5.40                  | 100                        | 100                    |
| childfund.org        | N/A                    | 0                     | N/A                        | N/A                    |
| unicef.org           | 100                    | 0                     | 100                        | 100                    |
| childrenshealthfund.org | 100             | 9.09                  | N/A                        | 100                    |

Table 5: Percentage of detected images that are invisible based on domain of origin (from EU IP address)

| Domain               | % AEs server/delivery | % content site/domain | % web analytics site/domain | % tracking site/domain |
|----------------------|------------------------|-----------------------|----------------------------|------------------------|
| thearsusa.com        | 93.92                  | 15.38                 | 100                        | 80                     |
| reverseimage.net     | 95.24                  | 0                     | 100                        | 93.75                  |
| britains.com         | 100                    | 17.76                 | 100                        | 100                    |
| howstuffworks.com    | 100                    | 0                     | N/A                        | N/A                    |
| citationmachine.net  | 93.94                  | 14.29                 | 100                        | 85.95                  |
| bintendo.com         | N/A                    | 1.05                  | 98.95                      | 100                    |
| legianflagends.com   | 100                    | 0                     | 100                        | 100                    |
| bulbagarden.net      | 0                      | 100                   | N/A                        | N/A                    |
| nintendo.com         | 100                    | 16.67                 | 100                        | 100                    |
| es.com               | N/A                    | 16.67                 | N/A                        | N/A                    |
| amextravel.com       | N/A                    | 0.25                  | 100                        | N/A                    |
| nudg.com             | N/A                    | 3.33                  | N/A                        | N/A                    |
| pokemons.com         | N/A                    | 3.33                  | N/A                        | N/A                    |
| chapelorgan.com      | N/A                    | 0                     | 100                        | 100                    |
| foopets.com          | 100                    | 0                     | 100                        | 66.67                  |
| children.org         | 100                    | 17.39                 | 100                        | 100                    |
| savechildren.org     | 100                    | 34.78                 | 100                        | 100                    |
| childfund.org        | 100                    | 4                     | 100                        | 100                    |
| unicef.org           | 100                    | 15.98                 | N/A                        | 100                    |

Table 6: Percentage of images with cookies based on domain of origin (from US IP address)
Table 7: Percentage of images with cookies based on domain of origin (from EU IP address)

![Table with data](image)

Figure 2: Partial histogram showing the number of websites from Table 1 containing images from each particular third-party company (from US IP address)

![Histogram](image)

Figure 3: Partial histogram showing the number of websites from Table 1 containing images from each particular third-party company (from EU IP address)

![Histogram](image)