2015 GPEN Sweep – Children's Privacy

Summary Observations

Many websites and apps targeted at, or popular among, children are collecting personal information without offering kids and their parents adequate protective controls to limit the use and disclosure of such personal information, or a simple means of deleting an account permanently. That said, one third of websites or apps that were swept demonstrated that they could be successful, appealing and dynamic without the need to collect any personal information at all.

Tombstone Data

Participating Data Protection Authorities:	29
Sites and apps:	1494

***Methodology Note**: Not all Data Protection Authorities ("DPAs") reported on every reporting field. As a result, the statistics for this Sweep were developed based on the actual data received for a reporting field as a percentage of those apps/websites swept by those DPAs that reported on that field. In order to maintain methodological integrity, percentages derived from separate reporting fields with non-identical denominators were not, and cannot be, aggregated for reporting purposes.*

Sweeper Comfort (Indicator 4)

Sweepers indicated that approximately 41% of websites and apps reviewed left them uncomfortable. In general, sweepers indicated that they would not want a child to use these sites or apps. DPAs were concerned about a variety of issues, including:

- Inadequate or nonexistent privacy policies, or lengthy and complex privacy policies
- Over-collection of information:
    - For example, collection of exact date of birth instead of simply the year/month of birth to verify a user's age
- Failure to use simple language, or failure to present warnings that children could easily read and understand (78% of sites/apps swept)
- Disclosure of user information to third parties, in some cases for vague or unspecified purposes:
    - Sweepers indicated that 51% of sites and apps stated that they may disclose user information to third parties
- Certain "virtual worlds" that facilitate contact with kids:
    - For example, through a free text chat function. Sweepers reported examples of such functions being unmonitored, allowing kids to potentially disclose their personal information to strangers via free-text. Sweepers also reported a similar issue whereby a website allowed children to post their drawings online, but failed to monitor drawings to ensure no personal information was included (like the child's name and address found in one example).

- The potential to be redirected to another website via advertisements (58% of sites/apps swept).

Several DPAs observed that, overall, websites and apps targeted at young children, presented a more protective privacy environment for children than those that were simply "popular" with children.

Collection of Personal Information (Indicator 1)

DPAs applaud the 33% of websites and apps targeted at, or popular among, children that apparently *do not* collect *any* personal information at all. Meanwhile, the remaining 67% of the sites and apps swept appeared to collect personal information. Of particular concern were the many websites and apps identified by sweepers that apparently collected those types of potentially sensitive personal information from children. In particular, DPAs were concerned that many websites and apps collected such information on a mandatory or optional basis: name (29% mandatory / 12% optional), date of birth (20% mandatory / 9% optional); phone number (12% mandatory / 10% optional); address (11% mandatory / 8% optional) and photos or video (9% mandatory / 14% optional).

The collection of this sort of personal information is particularly troubling given that for many sites and apps, sweepers saw privacy policies that in their view were unclear or generic, and provided little information about why a particular site or app was collecting personal information. As well, for certain sites and apps that presented privacy policies seemingly protective and robust on their face, upon closer review of the mechanics of the sites it became clear that the practices were not matching up to the rigour of the policies.

Protective Controls (Indicator 2)

DPAs saw some great examples of the use of protective controls. For example, one website provided users with pre-created avatars to use when navigating the site, removing the need for children to create their own avatars and to use their own information. Certain sites warned children not to use their real names when setting up an account. Some sites and apps with a chat function only allowed users to select words and phrases from a pre-approved list, instead of typing freely, so that children could not disclose their personal information inadvertently. One app automatically offered children under a specified age an alternative version of the app: this child-centric alternative appeared to collect and share less personal information compared to the adult-version of the app.

However, the fact that sweepers indicated only 31% of websites and apps swept had protective controls in place to effectively limit the collection of personal information from children raised concerns. Particularly troubling was the fact that on 58% of websites and apps swept, children could be redirected to another site or app, where the child could be asked to disclose their personal information. In certain cases, the redirection took place via an advertisement or contest which had the appearance of being part of the original site.

Also troubling was that, although many sites and apps claimed in their privacy policies to preclude access to children under a specified age, only 15% of websites and apps swept had age verification or gating to bar younger children from accessing the site or app. Sweepers also found that some of those controls did not function (e.g., a child indicating she was 10 years old could still access the site) and

others were only passive (e.g., a pop-up indicating that a child below a specified age should not access the site). Noteworthy, only 24% of sites and apps swept encouraged parental involvement.

Overall, DPAs believe that developers could do a much better job of boosting protective controls for sites and apps.

Deletion (Indicator 3)

Sweepers indicated that 29% of websites and apps swept provided an accessible means for deleting account information. All users, but particularly children, should have the ability to permanently delete their personal information. DPAs strongly urge developers of websites and apps which collect personal information to provide an easy and effective means for deletion.

Conclusion

In summary, websites and apps targeted at, or popular among, children contain a mixture of good and less desirable privacy practices. DPAs continue to encourage developers and owners of such sites and apps to improve their privacy practices by limiting the collection of personal information to only that which is necessary; tailoring communication to children; promoting parental involvement; incorporating effective protective controls; and providing accessible means for deleting account information.

Other

Separate from the aforementioned privacy issues, sweepers noted the inappropriate nature of certain advertisements on websites purported to be aimed at children, such as ads for dating websites or alcoholic beverages.

GPEN Privacy Sweep 2015 – Final Results

Total Number of Sites and Apps Examined: 1494
Total Number of DPAs: 29*

Indicators	Frequency	Percentage
1. Number of websites / apps examined which collect one or more pieces of personal information	999	67%
2. Number of websites / apps for which protective controls effectively limit the collection of personal data	332	31%
3. Number of websites / apps for which there is an accessible means for deletion of account information	304.5	29%
4. Number of websites / apps for which sweepers identified concerns	446	41%
Disclosure	**Frequency**	**Percentage**
Number of websites/apps which may disclose personal information	561	51%
Controls	**Frequency**	**Percentage**
Number of websites/apps which request some form of parental involvement	365	24%
Number of websites/apps with a parental dashboard	158	14%
Number of websites/apps for which the child could be redirected off the site	861	58%
Number of websites/apps that tailor protective communications to children	230	22%

Number of websites/apps which requested the following information:	Mandatory		Optional		Not Collected	
Data Requested	Frequency	Percent	Frequency	Percent	Frequency	Percent
Username	338	33%	165	12%	523	52%
Email	405	39%	211	15%	400	40%
Name	293	29%	175	12%	498	50%
Age/Grade	152	16%	108	11%	669	70%
Date of Birth	197	20%	122	9%	610	64%
Address	108	11%	119	8%	747	74%
Phone Number	117	12%	139	10%	715	71%
Photo/Video	95	9%	198	14%	696	69%
Chat Function	86	9%	244	19%	544	64%
Info of third party	56	5%	132	13%	758	75%
Cookies	615	67%	10	2%	178	24%
IP Address	467	51%	13	3%	245	35%
Unique Device Identifier	591	45%	22	5%	294	43%
Geo-location info	205	21%	31	4%	412	56%

Other	Frequency	Percentage
Number of websites/apps with third-party advertising	661	44%
Number of websites/apps with age verification / gating	212	15%

***Participants in the 2015 Sweep**

Argentina	*National Directorate for Personal Data Protection of Argentina*
Australia	*Office of the Australian Information Commissioner*
Australia, Victoria	*Office of the Commissioner for Privacy and Data Protection(CPDP)*
Belgium	*Privacy Commission of Belgium*
Canada	*Office of the Privacy Commissioner of Canada*
Canada, Alberta	*Office of the Information and Privacy Commissioner of Alberta*
Canada, British Columbia	*Office of the Information and Privacy Commissioner for British Columbia*
Canada, Quebec	*Commission d'accès à l'information*
China, Hong Kong	*Office of the Privacy Commissioner for Personal Data, Hong Kong*
China, Macao	*Office for Personal Data Protection, Macao*
Colombia	*Superintendence of Industry and Commerce of Colombia*
Estonia	*Estonian Data Protection Inspectorate*
France	*Commission Nationale de l'Informatique et des Libertés*
Germany, Bavaria	*Data Protection Supervisory Authority of Bavaria*
Germany, Berlin	*Berlin Data Protection Commissioner*
Germany, Hessen	*Data Protection Commissioner of Hessen*
Gibraltar	*Gibraltar Regulatory Authority*
Ireland	*Office of the Data Protection Commissioner*
Israel	*Israeli Law, Information and Technology Authority*
Italy	Garante per la protezione dei dati personali (*Italian Data Protection Authority)*
Korea	*Korea Internet and Security Agency*
Mexico	*Federal Institute for Access to Information and Data Protection*
Morocco	*La Commission Nationale de contrôle de la protection des Données à Caractère Personnel (CNDP)*
New Zealand	*Office of the Privacy Commissioner*
Norway	*Norwegian Data Protection Authority*
The Netherlands	*College Bescherming Persoonsgegevens (Dutch Data Protection Authority)*
United Kingdom	*United Kingdom Information Commissioner's Office*
United States	*Federal Communications Commission*
United States	*Federal Trade Commission*