December 2018

Digital Life Newsletter For Parents

Dear Parents and Guardians,

This month's issue deals with Posting Information About Your Child Online.
I hope you find it helpful.

Olga Garey
WHS School Library Media Specialist

This article from thenextweb.com deals with unwanted consequences of posting information about your child online.

It's not only people who would form opinions, preconceptions, and narratives around your child,it's the Googles, Facebooks, Amazons, Epsilons, and all the thousands and thousands of data-collecting companies that create profiles around our online personas and the relationships we have with other people, things, and ideas.

A report named *Who knows what about me?*, published by the UK's Children's Commissioner sets out hitting some brass tack stats: "by the age of 13, parents have posted 1300 photos and videos of their child to social media." What's worse than that number, is the fact that people tend to share pictures on momentous occasions, inadvertently giving away personal information about their child.

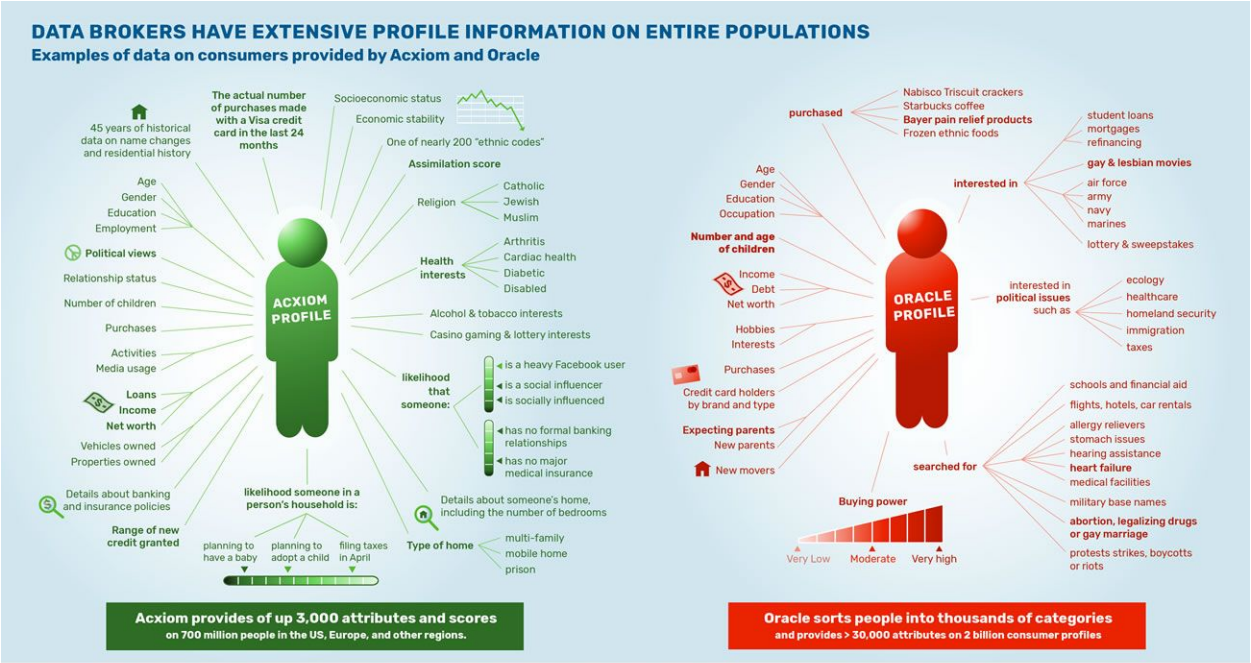
Giving it all away

Sharing a picture on the child's birthday, for example, tells advertisers when its birthday is. And if you forget to turn off location data, they'll know where he or she lives.

If it's a birthday party elsewhere, it can tell the advertiser what they like – i.e. dinosaurs in the Natural History Museum, or mummies, or royal offspring, or Disney.

And don't forget "'first day at school' photos, which often unintentionally reveal the child's location or identity through details such as school logos and street signs," as the report states.

What many people (choose to) forget, is that sharing a picture on Instagram or any other service sets off a mechanism that slurps up the data contained in that in picture – who's on it, where it is, what device it was taken on, the relationship of the people in it, and on, and on – slices it up, and shares it with whatever company finds that data useful.



Credit: CrackedLabsAn infographic made by CrackedLabs on what info some data brokers collect on you and yours

Some of it might end up in the databases of the huge companies that compile commercially exploitable profiles of people. Some of it might be used to target the parents with ads for toys the child might be interested in. Some of it might be saved, lying dormant until it's needed by an insurance company, or a bank, or to set bail.

This type of data, that is not directly given to social platforms, is labeled in the report as ‘given off’ or ‘inferred’ data. The data is not given explicitly, but extracted by companies like Facebook, Instagram (which belongs to Facebook), or Google from the innocent-seeming posts you might share about your child.

All of that is combined with other data already in the system to paint a digital picture of your child, which might not be completely accurate, but is still used by many companies to make decisions about them.

Everything you share “might have real, long-lasting implications on children’s lives,” the report states.

We’ll get to the cons of those real, long-lasting implications later, because not everything is terrible and there might even be some benefits to be had from selectively sharing data.

The good, briefly

Not all data are created equal. Pictures shared on Instagram are data, but so are anonymized health records. Data collectors are not all cut from the same cloth either.

In one example, local authorities in the UK collected data from children and parents to use predictive analytics to successfully flag children at risk of abuse to social workers, the Guardian reports. This could be seen as a ‘good’ use of data – if you can peek past the vaguely Orwellian veil.

But as with any other data collection, data collected for good can leave a record that might be at best hard to shake, and worst, completely abused.

The bad, extensively

The CCO report notes that they heard accounts of criminals collecting information shared by parents – date of birth, home address, and full name – that they used to apply for fraudulent loans and credit cards once the child turns 18.

Answers to common security questions like a mother’s maiden name, the name of first pets, schools, or cars are also increasingly easily gleaned from ‘sharenting’, as the report calls the tendency of some parents to share everything about their kids’ lives.

Now, the cases above might be extreme and rare, but what ‘legal’ entities like Facebook and Instagram can do might be even more concerning – because you can’t really report them to the police.

The CCO report details profiling of children based on shared data as a serious long-term risk:

Profiling is a process in which data about a person is analyzed using algorithms and machine learning "to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."

It states these profiles can be used to determine preferences, predict behavior, and make decisions about individuals. In the most innocent case, this can be useful for advertisers to decide what products to show a kid (or their parent) and when – like around their birthday, the date of which you conveniently shared.

In more serious cases, profiling can be used to determine whether someone can apply for a mortgage, a certain health insurance, universities, or even bail.

It all adds up

Profiles on individuals aggregate information from all kinds of different sources – sometimes starting even before the child is born – so everything you do, however innocent it might seem, just adds up.

To top it off, some machines that do analyses on personal data (or any data) are, as the report calls it, "unfairly reductive," meaning they don't take kindly to nuances, excuses, or inconsistencies. A 'bad behavior' datapoint, like an unpaid bill, might flag you as unworthy of credit, even if you're a model human otherwise.

All information in this article was taken from the following Website.

https://thenextweb.com/lifehacks/2018/11/12/dont-post-your-kid-online/?utm_source=pocket&utm_medium=email&utm_campaign=pockethits