How parents threaten children's online privacy

May 13 2015

Credit: Petr Kratochvil/public domain

Most parents go to great lengths to keep their children safe online—but what if parents themselves, through the simple act of posting photos to Facebook and Instagram, are putting their own kids at risk every day?

Researchers at the New York University Polytechnic School of Engineering and NYU Shanghai have released a study showing that

parents' habits on popular social media sites may allow third parties to easily obtain their children's identities and other sensitive information. Their paper, "Children Seen but Not Heard: When Parents Compromise Children's Online Privacy" will be presented at the International World Wide Web Conference in Florence, Italy, on May 22, 2015.

The paper's primary investigator, Keith W. Ross, dean of engineering and computer science at NYU Shanghai and the Leonard J. Shustek Professor of Computer Science at the NYU School of Engineering, explained that he and his colleagues explored the degree to which parents' online behavior may compromise their children's privacy. Through analysis of publicly available page photos from Facebook, combined with public records such as voter registrations, the researchers were able to quickly obtain personal information about children, including their names, birthdays, and even home addresses.

First, the research team crawled the public profiles of about 2,400 adult Facebook users in a single East Coast suburban town, deploying off-the-shelf age prediction software to identify children's faces in photographs posted on these pages. They instructed the software to focus on children estimated to be under age seven, and the results yielded more than 2,200 photos of children in this age group. By using machine learning software, researchers were immediately able to deduce the child's name from public comments in 26 percent of the photos. Among all accounts where a child's photo was present (807 accounts), they were able to determine the child's last name and, in half of those cases, the child's first name as well.

By matching names from Facebook with public voter registration records in the town, the team was able to determine the parent's birthday, home address (and hence the child's home address), and political affiliation.

Tehila Minkus, lead author of the paper and doctoral candidate at the NYU School of Engineering, explained the goal of the study. "Our intention was not to publicly expose sensitive information about children, but rather to raise public awareness about the results of parental oversharing," she said. "The techniques we used to automate this search and obtain information would be well within the scope of a data broker, online service provider, surveillance organization, or even malicious strangers," she says.

The researchers also conducted an online poll of parents who use Facebook to determine their attitudes and practices when it comes to posting images of children online. Among 357 respondents, 82 percent said they had posted a picture of their child at least once, 77 percent said they had mentioned their child's name in a post on Facebook, and 54 percent said they had referenced their child's birthday or actual date of birth. Nonetheless, when asked about their concern for their children's privacy online, the majority of respondents ranked their worries for their children's privacy at about the same level as their own privacy— about 3.75 on a scale of 1 to 5.

The team extended the investigation to Instagram; unlike Facebook, all Instagram posts and profiles are public by default and can be followed by anyone. By searching for parenting-related hashtags, they identified more than 1,000 accounts of likely parents, which featured more than 6,000 photos of young children. About 63 percent of the accounts included a child's name in at least one photo, and 27 percent mentioned a birthday. Nearly 20 percent of parents posting to these accounts referenced both their child's name and birthday.

"This aspect of children's privacy hasn't been measured on a large scale," explained NYU Shanghai undergraduate student Kelvin Liu, who was also part of the research team. "By demonstrating just how much information can be gained about a child through adults' online activities,

we hope to spur parents to take precautions to minimize their children's exposure online."

Minkus, Liu, and Ross outline several risk-reduction recommendations in the paper, including suggestions for Facebook and for parents.

For Facebook, they recommend a privacy-preserving mechanism that prompts users to consider restricting their sharing behaviors when it comes to images of children. If a child's face is detected in a photo, a message could be displayed to encourage the user to select more private settings for the post. The site could also implement a policy to automatically restrict photos containing children to a more private sharing setting.

For parents, the suggestions are simple but powerful: increase privacy settings to limit the audience for images of children; make Instagram accounts private; think twice before sharing potentially embarrassing images of children; avoid sharing a child's name or other details; and consider photo encryption software that limits visibility to all but those with the key.

While Ross acknowledges that overall risk to children's physical safety due to online exposure is likely to be low, he does not minimize the potential impact of digital dossiers on millions of children. "Adults on Facebook and Instagram have chosen to expose information online, but their children have given no such consent," Ross says. "We aren't telling parents to stop posting images of their children online, but we are asking them to consider that this does reduce their child's privacy later in life, and to take simple steps to minimize those risks."

Provided by New York University