5

Recommendations for Protecting Your Child's Privacy Online

By John Dunnery

Parenting has never been easy. Parents have the huge responsibility of protecting their growing children from all sorts of dangers. Yet most parents have developed the necessary skills to monitor the threats that have always existed in the home, the neighborhood, and the school environment.

However, the Internet has added a whole new set of dangers. Unfortunately, many adults are still not fully aware of the threats that exist online – which is somewhat understandable, as those threats are continually evolving. Consequently, many parents have not yet learned to monitor the online environment and protect their children from the related dangers.

One basic issue is privacy. The repercussions of a loss of privacy through online activity are becoming more and more serious. Adults can freely choose to accept such repercussions when they post information about themselves online. However, small children have no choice about what their parents post about them.

Here are five recommendations for protecting your child's privacy online. While they may seem extreme, there are sufficient reasons for each cautionary statement.

1 **Consider restricting the use of your child's full name online.**
The name is the key to all the identification activities of websites, marketers, and individuals. Providing your child's name online is like putting a label on a file folder into which other information can then be inserted. Instead of using a full name in a blog post or in a photo tag, you could perhaps write "my son" or "our younger daughter."

2 **Avoid posting numerous close-up photos of the child's face.**
Again, this advice may seem extreme or unwarranted. However, the reality is that facial recognition technology has advanced significantly. Indeed, applications already exist that allow users to identify individuals by scanning the face in online photos and comparing the data to that from other scanned images.

3 **Avoid revealing the child's address, either in text or in photos (for example, where your street number is shown in the photo background).**
The address provides another key coordinate that allows websites, marketers, and individuals to identify – or stalk – your child.

4 **Don't post photos of your child that are excessively revealing.**
That cute photo of the baby in the bathtub or the toddler running through the backyard sprinkler may, unfortunately, be discovered by a pedophile.

5 **Consider restricting the posting of other identifying information, such as the child's school, church, or sports team.**
All such pieces of data serve as clues that can be used to identify a child.

The goal of all these recommendations is to prevent the imprint of a large online footprint representing your child. The assumption behind the recommendations is that each person should have the freedom to shape his or her own online identity as the person grows into adulthood.

If parents post large amounts of identifying information about their growing child online, the young adult is forced to carry the weight of this – all the photos, comments, and associations – throughout life.

Once something is posted online, there is no way to retrieve or erase it. That cute photo of the baby in the bathtub or the anecdote about the pubescent teen will follow your child throughout his or her life – and may attract unwanted interest or attention.