

## **Inside 1to1 Privacy**

**Date: 09/03/2008**

**Issue: September 3, 2008**

**People: Don Peppers & Martha Rogers, Ph.D.**

**Content Channel: Emerging Trends**

### **Photo Tagging Portends New Frontier for Privacy Pros**

If privacy officers succeeded in compelling every corporation and government around the world to implement the most stringent privacy controls, would the privacy of the world be intact? The advent of photo tagging suggests this answer is No--and the trend raises fundamental questions about the future role of the corporate privacy officer.

According to ZDNet, people worldwide took 50 billion digital photos in 2007, roughly 8 for every person alive. The vast majority of these photos are e-mailed to family or friends, or uploaded to Web sites where only friends and family are given access. MySpace reports that its 110 million users have uploaded 1.5 billion images to their sites. Facebook says its 90 million users add 14 million photos to the platform each day. Within these areas of life, people's privacy is at peace, because they are in control of their information.

The rise of photo tagging--the appending of personal information to digital images--is quickly changing the balance of privacy, however. The most common and benign way that photo tagging occurs is when people voluntarily tag photos of themselves. After I posted my portrait to my Facebook profile, for example, that image now displays whenever someone searches Facebook for my name.

More than just a name can be tagged on digital photos. Some digital cameras now come with GPS accessories that add geocode coordinates to photos. The metadata associated with these exchangeable-image file (exif) files stay attached to the image when it gets uploaded to a Web site. Sony, for example, sells a GPS Tracker Device that adds location data to photos and videos, and then plots them onto a Google map matching the longitude and latitude coordinates of the exif file.

This otherwise harmless and delightful innovation starts to open new privacy horizons when photo tagging becomes "social tagging." Social tagging occurs when you append your own tag to someone else's picture. If I uploaded a photo to my account on Yahoo!-owned Flickr--where more than two billion photos are now stored, and five million added each day--I could add to the photo a tag that says "Jeff Johnson" and "Wild Party" and make it publicly available. Jeff wouldn't know I tagged him in the photo unless someone told him, and would have no easy way of removing his photo.

Automatic social tagging has upped the privacy ante. Based on technology first developed at

Stanford by Professors Jia Li and James Wang, autotagging happens when software automatically appends tags to photos based on the geocode metadata or facial-image coordinates. As people upload images to alipr.com, the professors' longtime project, its backend engine uses a library of English words to guess which tags should apply to the photos. As this project matures, it promises to broaden and accelerate the number of tagged images in its archives.

Others are already pointing their autotag guns outward toward the 85 billion Web pages on the Internet. The banner on PolarRose.com leaves no doubt about its goals: "35,329,716 photos discovered, 219,076 people named." In addition to user-uploaded images, the Swedish Web site searches the Web for photos, matches faces with previously indexed images, and tags the new images.

The end result of these isolated ventures is an emerging confluence of Web sites and technologies that is larger than the sum of its parts. In the not-too-distant future, these initiatives could produce the geocoded history of photos of you, of people who look like you, and of people erroneously tagged as you, for anyone who searches Google with your name and "image" as keywords. And, since no one corporation or government agency controls the entire playing field, there are at this point few avenues of recourse for people whose privacy has been forever exposed by this phenomenon.

How will people react to an escalating likelihood of being autotagged? Some, including the Web 2.0 generation that never had high expectations of privacy, may change nothing about how they live. Others who are more cautious will withdraw from digital-photo sharing and try to avoid being photographed.

But many who occupy the middle tier of society--the "privacy pragmatists" who Dr. Alan Westin says will make case-by-case decisions about their privacy--may increasingly patronize companies who make it easy for them to navigate the trade-offs between privacy and convenience.

If Web 2.0 starts to routinely expose and harm innocent bystanders, corporate privacy officers will encounter a new opportunity to redefine their roles. Today, many organizations view their CPOs as internally focused--the people who keep the organization out of the headlines by keeping them in compliance with the necessary policies and regulations.

But for companies whose revenues depend on public trust in the online world, the CPO may need to become more externally focused. Tomorrow's CPO may need to help protect the online ecosystem and assist with products and services that guide consumers safely through it.

*Look for additional ubiquitous identification series installments in future issues of Inside 1to1: Privacy.*

*You can reach Don Peppers and Martha Rogers at [dpeppers@1to1.com](mailto:dpeppers@1to1.com) or [rogers@1to1.com](mailto:rogers@1to1.com).*