Online and Overexposed:
Consumer Privacy, the FTC, and the Rise of the Cyberazzi
Remarks of FTC Chairman Jon Leibowitz as Prepared for Delivery
National Press Club, Washington, D.C.
October 11, 2011

Thank you Jeff, and let me also extend my thanks to the many other organizers of this event. I'm happy to be here. Jeff will be announcing a new study today, which we haven't yet seen, but I am certain it will move us toward the goal we all share – and it seems to me that goal is shared by many businesses – protecting consumer privacy while ensuring a cyberspace that generates the free content we've all come to expect and enjoy.

Based on reading we have been doing over the last couple of weeks, most of it picked up while waiting in line at the grocery store, we have concluded: Kirstie Alley could have had gastric bypass surgery, and Kim Kardashian almost definitely had a butt lift. Blake Lively and Leo diCaprio's short-lived relationship seems faker than – well, Kim Kardashian's rear end. And it doesn't look good for Ashton and Demi; she been nowhere near the set of Two and a Half Men.

Thank goodness for the paparazzi. And really, who cares that, of the 1000 words each of their pictures is worth, at best only about 500 are true? Public figures choose to make their livings monetizing their identities; in a free market, it is hardly surprising that photographers and gossip rags want to get in on the action.

It would be a different story, of course, if the paparazzi turned their lenses on those of us who don't have jobs treading the red carpet – if they snapped photos of us in what we thought were our private moments and then sold them without our permission, the resulting montage a detailed and perhaps damaging portrait of our selves.

But you could make the case that this is exactly what happens every time we access the Internet. A host of invisible cyberazzi – cookies and other data catchers – follow us as we browse, reporting our every stop and action to marketing firms that, in turn, collect an astonishingly complete profile of our online behavior. Whenever we click, so do they.

One day you might print out a CDC fact sheet on alcoholism to help your son with a project for health class.

purpose, store it securely, keep it only as long as necessary to fulfill its legitimate business need, then dispose of it safely. The more sensitive the data, the stronger the protections should be. To its credit, much of industry is embracing this approach – even before we issued the draft report.

Second, transparency. Any companies gathering information online need to tell consumers what's going on. And by this, I do not mean another three-point font, ten-page document written by corporate lawyers and buried deep within the site. I asked our staff to look at data disclosures on mobile devices; one form took 109 clicks to get through, and the staffer who discovered that is probably the only one who ever made it to click number 109.

Transparency is not an unreasonable request. My daughters can go to any of a number of retail clothing websites, and, with one click, see a clear description of a pair of pants – color, sizes, fit, customer reviews, shipping options. One more click – that's a total of 2, not 109 – and they can choose exactly the pants they want, in their sizes and favorite colors, shipped where they want them. Put the guy who designed that page on the job of presenting a meaningful disclosure and consent form.

Third, choice. Consumers should have streamlined and effective choices about the collection and use of their data. That includes choices about when, why, and how cyberazzi follow them into cyberspace. To that end, we proposed a "Do Not Track" mechanism that will allow consumers to decide whether to share information about their browsing behavior. We envision a system consumers can find and use easily and one that all companies employing cyberazzi must respect.

A vision of Do Not Track bears some similarities to the successful Do Not Call program. Now with more than 200 million registered phone numbers, Do Not Call has brought some peace and quiet to Americans' dinner hour; no wonder Dave Barry called it the "most popular federal concept since the Elvis stamp." But unlike Do Not Call, the FTC does not think Do Not Track should be administered by the government. We hope different sectors of industry will work collaboratively to give consumers choices about how and when they are tracked online.

A number of leading online businesses have responded to our call for Do Not Track. Microsoft, Mozilla, and Apple have implemented their own Do Not Track features, and we remain hopeful that Google will join them. A half dozen advertising networks pledged to honor the Mozilla Do Not Track header. And that, I suspect is only the tip of the online advertising iceberg.

The FTC's chief technologist, the wonderful Ed Felten, is participating in the W3C, a key Internet standards-setting body defining technical standards for Do Not Track. In this and other similar endeavors, the FTC supports standards that provide persistent and effective choices but do not interfere with the normal data flows necessary to a thriving Internet. We think this balance can be struck without too much difficulty.

To its credit, the online advertising industry is also focusing on consumer choice architecture. The Digital Advertising Alliance, a coalition of media and marketing associations, is making progress on its "Ad Choices" icon, which consumers can click to opt out of targeted advertising. We are encouraging the industry to partner with browser vendors to ensure that that

consumer choice is persistent and effective, and that it encompasses not just the advertising the consumer sees, but also the information about the consumer that the advertisers – and others – collect.

Of all the recommendations in the December privacy report, Do Not Track has probably received the most exposure: in fact, it has probably been overexposed, leading to a fuzzy picture of exactly what Do Not Track will do.

To be clear: Do Not Track will not end behavioral advertising, the targeted marketing that funds a wealth of free online content. The FTC has no intention of pulling a Sean Penn on the cyberazzi. Many, if not most, consumers prefer targeted ads: do you really want to scroll through a leggings' montage from Forever 21 when you can instead open your computer right to the announcement of LL Bean's annual chinos' sale?

At the FTC, we are agnostic as to how Do Not Track comes about: it doesn't matter what technology backs the system, so long as it works. But no .00 TD.000Tc-.t

You have probably heard about our cases against Google for its Buzz social network, and against Twitter for data