**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. Click. Or you order a box of your mother's favorite candy to take her when you go visit. Click. Or you buy the book "The Winner's Guide to Casino Gambling" as a raffle prize for your church's Las Vegas night. Click.

You know you are a dutiful parent, but a potential employer could see a boozy job applicant. You know you are a thoughtful daughter, but a health insurer could see a destined diabetic. You know you are a generous member of the community, but a loan officer could see a risky gambler.

Click. Click. Click.

It is true that paparazzi know who their celebrity subjects are while the cyberazzi may not have linked – at least not publically – our identities to the profiles they are building. But that could happen; disturbingly, it may even become common practice.

Often the buyers of these cyber-snaps are companies that target internet advertising to your particular interests, a beneficial – or at worst innocuous – marketing practice that helps support free web content. But your tracked information doesn't have to stop there; it could be traded throughout an invisible lattice of companies, snowballing into an exhaustive profile of you available to those making critical decisions about your career, finances, health, and reputation.

Of course, most online advertisers are nothing like paparazzi; many companies have strong privacy policies protecting consumers. But we are not presenting a digitally altered picture of the situation. Once you enter cyberspace, software placed on your computer – usually without your consent or even knowledge – turns your private information into a commodity out of your control. And keep in mind: as my former colleague Republican FTC Chairman Debbie Majoras used to say, your computer is your property.

At the FTC, we want you to get that control back. We've been safeguarding privacy since long before the cyberazzi focused their wide angles on the public. Our goal: to stay one step ahead of technology as it races along, finding better hiding places, stronger lenses, and more means to record and store your every move.

The FTC has been working on consumer privacy since the 1970's. In the early days of the Internet, businesses posted privacy policies, which they – and we – expected consumers to read and understand. We soon learned that both were unlikely. Who is going to examine a legal document as long as the Code of Hammurabi, when all that stands between them and free shipping is checking the little box – often conveniently pre-checked for you – that says "I consent?"

This is not meaningful privacy protection for consumers in cyberspace. With that same space expanding exponentially to allow more and more data collection that is more and more often invisible to consumers, the Commission is looking for another way allow consumers to cap the lenses of the cyberazzi.

Looking to how celebrities handle paparazzi doesn't provide much guidance: Matt Damon suggested never doing anything in public of any interest. Jude Law counseled tossing root vegetables at the stalkers. The Commission decided to take instead a position that, while organic, was not so in the vegetative sense: In a preliminary report issued by staff in December 2010, we proposed a new framework for safeguarding consumers' personal data flexible enough to allow both businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace. We expect to issue a final report in the coming months.

The report puts forth three principles to guide policymakers and industry as they, we hope, work together to protect privacy online.

First, companies in the business of collecting, storing, and manipulating consumer data need to build privacy protections into their everyday business practices – we call this "privacy by design." Companies that collect consumer data should do so only for a specific business

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 matter what, it should be easy to use and easy to find.

Industry's interest in developing tracking choices for consumers is heartening; they have the experience and knowledge to draft a flexible, workable approach quickly. If they do not, however, there are signs that Congress might impose a Do Not Track system of its own design on the private sector.

When it comes to the tracking of adults, we believe that, with good faith and full disclosure on all sides, industry will strike a reasonable balance between consumer privacy and the information needs of online advertisers. But the cyberazzi do need to stay away from our kids – at least without parental consent.

The FTC protects children's privacy online through COPPA – the Children's Online Privacy Protection Act – and our Rule implementing the Act. The Rule requires operators of websites and online services directed at children under the age of 13, as well as other online sites and services that knowingly collect information from children under 13, to obtain parental consent before collecting personal information from children.

Last month, we proposed updates to the COPPA Rule to keep pace with both rapid technological change – such as geo-location services, social networks, and tracking cookies – and even more rapid evolution of tech-savvy kids' ability to outwit parental consent. We are seeking public comment on the proposed amendments and will take into account all the comments we expect to receive – from consumer groups, advertisers, children's website operators, and technologists.

While we at the FTC are proud of our work on privacy policy and rules, we are primarily an enforcement agency. Over the last ten years, we've brought more than 100 spam and spyware cases, and 79 Do Not Call cases with over $580 million in civil penalties ordered. We've also brought more than 30 data security cases, most of which ended in companies adopting comprehensive security programs and undergoing independent audits.

You have probably heard about our cases against Google for its Buzz social network, and against Twitter for data security lapses that allowed hackers to gain control of accounts – one sending a tweet purportedly from President Barack Obama offering the chance to win $500 in free gas, and another purportedly from Britney Spears making disturbing comments about her own anatomy. Decorum prevents me from relaying those unauthorized Britney Spears postings.

But you may not have heard about our action against a company called Chitika. Though it's not a household name, Chitika has a sizeable presence behind the scenes delivering targeted online advertising. It offered consumers the chance to opt out of tracking but did not disclose that the opt-out was good for only ten days. To settle FTC charges, Chitika agreed to stop making misrepresentations and only supply real opt-outs that last at least five years.

Here, again, we capped the overly long lens of this cyberazzi. And Chitika has also gone one step further: it has agreed to honor the Do Not Track signal that browser companies like Mozilla have implemented.

Today we are announcing a privacy case against a company called Frostwire, which offers mobile P2P software used by hundreds of thousands of consumers. We charged that Frostwire shared its users' personal cellphone pictures and other data without their consent. Frostwire's default settings, which were extremely difficult to change, had been automatically revealing private photos and videos taken with users' phones to other P2P users around the world – in effect turning all its clients into both unwitting paparazzi and unaware paparazzi victims.

We now have a settlement order against Frostwire prohibiting default settings that automatically share the files users have created. Had Frostwire practiced privacy by design, as our 2010 staff report suggested, it would have built into the software consumers' reasonable expectations that their private photos stay private, and would have avoided a run-in with our agency's team. Had it embraced the transparency principle, it would have provided clearer information to consumers who could make choices about the sharing of personal content like photos and videos.

The bottom line is this: cyberspace need not be a privacy-free zone, a place where, without our consent or knowledge, our every online click is tracked and recorded with the intensity of a "National Enquirer" photographer trying to catch Justin Bieber on a bad hair day. The FTC is committed to a thriving and innovative Internet through policy recommendations for self-regulatory efforts and strong enforcement. By working with all of you in the audience today, I believe we can keep cyberazzi lenses focused on willing subjects and ensure the right of all citizens to choose the public faces we present to the world.