Jeff Bezos Protests the Invasion of his Privacy as Amazon Builds a Sprawling Surveillance State For Everyone Else

Glenn Greenwald

The National Enquirer has engaged in behavior so lowly and unscrupulous that it created a seemingly impossible storyline: the world's richest billionaire and a notorious labor abuser, Amazon CEO Jeff Bezos, as a sympathetic victim.

On Thursday, Bezos published emails in which the Enquirer's parent company explicitly threatened to publish intimate photographs of Bezos and his mistress, which were apparently exchanged between the two through their iPhones, unless Bezos agreed to a series of demands involving silence about the company's conduct.

In a perfect world, none of the sexually salacious material the Enquirer was threatening to release would be incriminating or embarrassing to Bezos: it involves consensual sex between adults that is the business of nobody other than those involved and their spouses. But that's not the world in which we live: few news events generate moralizing interest like sex scandals, especially among the media.

The prospect of naked selfies of Bezos would obviously generate intense media coverage and all sorts of adolescent giggling and sanctimonious judgments. The Enquirer's reports of Bezos' adulterous affair seemed to have already played at least a significant role, if not the primary one, in the recent announcement of Bezos' divorce from his wife of 25 years.

Beyond the prurient interest in sex scandals, this case entails genuinely newsworthy questions because of its political context. The National Enquirer was so actively devoted to Donald Trump's election that the chairman of its parent company admitted to helping make hush payments to kill stories of Trump's affairs, and received immunity for his cooperation in the criminal case of Trump lawyer Michael Cohen, while Bezos, as the owner of the steadfastly anti-Trump Washington Post, is viewed by Trump as a political enemy.

All of this raises serious questions, which thus far are limited to pure speculation, about how the National Enquirer obtained the intimate photos exchanged between Bezos and his mistress. Despite a lack of evidence, MSNBC is already doing what it exists to do – implying with no evidence that Trump is to blame (in this case, by abusing the powers of the NSA or FBI to spy on Bezos). But, under the circumstances, those are legitimate questions to be probing (though responsible news agencies would wait for evidence before airing innuendo of that sort).

If the surveillance powers of the NSA, FBI or other agencies were used to obtain incriminating information about Bezos due to their view of him as a political enemy – and, again, there is no evidence this has happened – it certainly would not be the first time. Those agencies have a long and shameful history of doing exactly that, which is why the Democratic adoration for those agencies, and the recent bipartisan further empowerment of them, was so disturbing.

Indeed, one of the stories we were able to report using the Snowden documents, one that received less attention that it should have, is an active NSA program to collect the online sex activities, including browsing records of porn site and sex chats, of people regarded by the U.S. Government as radical or radicalizing in order to use their online sex habits to destroy their reputations. This is what and who the NSA, CIA and FBI are and long have been.

If Bezos were the political victim of surveillance state abuses, it would be scandalous and dangerous. It would also be deeply ironic.

That's because Amazon, the company that has made Bezos the planet's richest human being, is a critical partner for the U.S. Government in building an ever-more invasive, militarized and sprawling surveillance state. Indeed, one of the largest components of Amazon's business, and thus one of the most important sources of Bezos' vast wealth and power, is working with the Pentagon and the NSA to empower the U.S. Government with more potent and more sophisticated weapons, including surveillance weapons.

In December, 2017, Amazon boasted that it had perfected new face-recognition software for crowds, which it called Rekognition. It explained that the product is intended, in large part, for use by governments and police forces around the world. The ACLU quickly warned that the product is "dangerous" and that Amazon "is actively helping governments deploy it."

"Powered by artificial intelligence," wrote the ACLU, "Rekognition can identify, track, and analyze people in real time and recognize up to 100 people in a single image. It can quickly scan information it collects against databases featuring tens of millions of faces." The group warned: "Amazon's Rekognition raises profound civil liberties and civil rights concerns." In a separate advisory, the ACLU said of this face-recognition software that Amazon's "marketing materials read like a user manual for the type of authoritarian surveillance you can currently see in China."

BuzzFeed obtained documents showing details of Amazon's work in implementing the technology with the Orlando Police Department, ones that "reveal the accelerated pace at which law enforcement is embracing facial recognition tools with limited training and little to no oversight from regulators or the public." Citing Amazon's work to implement the software with police departments, the ACLU explained:

> With Rekognition, a government can now build a system to automate the identification and tracking of anyone. If police body cameras, for example, were outfitted with facial recognition, devices intended for officer transparency and accountability would further transform into surveillance machines aimed at the public. With this technology, police would be able to determine who attends protests. ICE could seek to continuously monitor immigrants as they embark on new lives. Cities might routinely track their own residents, whether they have reason to suspect criminal activity or not. As with other surveillance technologies, these systems are certain to be disproportionately aimed at minority communities.

Numerous lawmakers, including Congress' leading privacy advocates, wrote a letter in July, 2018, expressing grave concerns about how this software and similar mass-face-recognition programs would be used by government and law enforcement agencies. They posed a series of

questions based on their concern that "this technology comes with inherent risks, including the compromising of Americans' right to privacy, as well as racial and gender bias."

In a separate article about Amazon's privacy threats, the ACLU explained that the group "and other civil rights groups have repeatedly warned that face surveillance poses an unprecedented threat to civil liberties and civil rights that must be stopped before it becomes widespread."

Amazon's extensive relationship with the NSA, FBI, Pentagon and other surveillance agencies in the west is multi-faceted, highly lucrative and rapidly growing. Last March, the Intercept reported on a new app that Amazon developers and British police forces have jointly developed to use on the public in police work, just "the latest example of third parties aiding, automating, and in some cases, replacing, the functions of law enforcement agencies — and raises privacy questions about Amazon's role as an intermediary."

Beyond allowing police departments to "store citizens' crime reports on Amazon's servers, rather than those operated by the police," the Amazon products "will allow users to report crimes directly to their smart speakers," an innovation David Murakami Wood, a scholar of surveillance, warned "serves as a startling reminder of the growing reach that technology companies have into our daily lives, intimate habits, and vulnerable moments — with and without our permission."

Then there are the serious privacy dangers posed by Amazon's "Ring" camera products, revealed in the Intercept last month by Sam Biddle. As he reported, Amazon's Ring, intended to be a home security system, has "a history of lax, sloppy oversight when it comes to deciding who has access to some of the most precious, intimate data belonging to any person: a live, high-definition feed from around — and perhaps inside — their house."

Among other transgressions, "Ring provided its Ukraine-based research and development team virtually unfettered access to a folder on Amazon's S3 cloud storage service that contained every video created by every Ring camera around the world." Biddle added: "This would amount to an enormous list of highly sensitive files that could be easily browsed and viewed. Downloading and sharing these customer video files would have required little more than a click."About the Ring surveillance in particular, the ACLU explained:

> Imagine if a neighborhood was set up with these doorbell cameras. Simply walking up to a friend's house could result in your face, your fingerprint, or your voice being flagged as "suspicious" and delivered to a government database without your knowledge or consent. With Amazon selling the devices, operating the servers, and pushing the technology on law enforcement, the company is building all the pieces of a surveillance network, reaching from the government all the way to our front doors.

Bezos' relationship with the military and intelligence wings of the U.S. Government is hard to overstate. Just last October, his company, Blue Origin, won a $500 million contract from the U.S. Air Force to help develop military rockets and spy satellites. Bezos personally thanked them in a tweet, proclaiming how "proud" he is "to serve the national security space community."

> Thank you to the @usairforce for your confidence in the @BlueOrigin team and our #NewGlenn rocket. We are proud to serve the national security space community and are

> committed to providing safe, reliable access to space for the nation. #GradatimFerociter pic.twitter.com/AeO3xXhnUi
>
> — Jeff Bezos (@JeffBezos) October 10, 2018

Then there's the patent Amazon obtained last October, as reported by the Intercept, "that would allow its virtual assistant Alexa to decipher a user's physical characteristics and emotional state based on their voice." In particular, it would enable anyone using the product to determine a person's accent and likely place of origin: "The algorithm would also consider a customer's physical location — based on their IP address, primary shipping address, and browser settings — to help determine their accent."

All of this is taking place as Amazon vies for, and is the favorite to win, one of the largest Pentagon contracts yet: a $10 billion agreement to provide exclusive cloud services to the world's largest military. CNN reported just last week that the company is now enmeshed in scandal over that effort, specifically a formal investigation into "whether Amazon improperly hired a former Defense Department worker who was involved with a $10 billion government contract for which the tech company is competing."

Bezos' relationship with the military and spying agencies of the U.S. Government, and law enforcement agencies around the world, predates his purchase of the Washington Post and has become a central prong of Amazon's business growth. Back in 2014, Amazon secured a massive contract with the CIA when the spy agency agreed to pay it $600 million for computing cloud software. As the Atlantic noted at the time, Amazon's software "will begin servicing all 17 agencies that make up the intelligence community."

Given how vital the military and spy agencies now are to Amazon's business, it's unsurprising that the amount Amazon pays to lobbyists to serve its interests in Washington has exploded: quadrupling since 2013 from $3 million to almost $15 million last year, according to Open Secrets.

Jeff Bezos is as entitled as anyone else to his personal privacy. The threats from the National Enquirer are grotesque. If Bezos' preemptive self-publishing of his private sex material reduces the unwarranted shame and stigma around adult consensual sexual activities, that will be a societal good.

But Bezos, given how much he works and profits to destroy the privacy of everyone else (to say nothing of the labor abuses of his company), is about the least sympathetic victim imaginable of privacy invasion. In the past, hard-core surveillance cheereladers in Congress such as Dianne Feinstein, Pete Hoekstra, and Jane Harmon became overnight, indignant privacy advocates when they learned that the surveillance state apparatus they long cheered had been turned against them.

Perhaps being a victim of privacy invasion will help Jeff Bezos realize the evils of what his company is enabling. Only time will tell. As of now, one of the world's greatest privacy invaders just had his privacy invaded. As the ACLU put it: "Amazon is building the tools for authoritarian surveillance that advocates, activists, community leaders, politicians, and experts have repeatedly warned against."