Statement from Amcrest CEO Adam Ravat

Thanks for reaching out for comment. Regarding the situation you describe, such an occurrence would have only been possible prior to our latest security updates and only in the rare instance where the original customer did not follow the correct return procedures and remove the camera from their cloud account and, at the same time, where a retailer re-sold such camera without first returning it to our facility for cloud reset in accordance with our vendor return policy. This would be similar to a situation where an original user does not wipe their data off of a smartphone before reselling it and a new user is able to access the original user's data. However, as soon as we were made aware of this issue in May of 2016 we immediately worked to release a firmware update as well as roll out additional cloud security enhancements which addressed the issue. Thus, on the basis of our latest security updates, even in instances where the correct return procedures are not followed such a potential security breach is no longer possible. We took the following measures to immediately address the issue and close the security loophole:

Firstly, we released a firmware update such that when a new user hard-resets their camera (a step that would be necessary in order to setup the camera for the new user), the camera would be automatically disassociated from any previous cloud account. Thus, in a situation where an original customer's cloud account was not removed, the new customer would only be able to setup the camera by performing a hard reset and thus by necessity would only be able to use the camera once it had been disassociated from the original user's cloud account. This essentially closes the loophole on a firmware level.

Secondly, as an added level of security, we upgraded the security requirements on our cloud such that the camera level password would be required in order to complete the connection between a camera and a cloud account. Thus, when a new user gets a previously used camera for the first time and is required to hard-reset the camera in order to use it, the hard-reset would result in resetting the camera level password. Thus, it would not be possible for a camera to connect to the original user's cloud account because the camera level password would no longer match. This essentially closes the loophole on the cloud level.

Furthermore, we would like to note that Nest had a similar problem and were also able to resolve the issue by security updates in a timely manner. Issues like these happen from time to time to big companies and small and we, like Nest and other true industry leaders, are committed to the security and privacy of our devices and will do everything within our power to address and solve any security or privacy issues once they are discovered. The real difference and takeaway here is that security issues are a reality in IoT and the most important thing for consumers to focus on are a manufacturer's commitment to security and its track record of resolving such issues in an effective and timely manner.

Aside from this particular question, our technology teams follow industry best practices for internet connected devices and our team is very proactive when addressing any potential security and privacy issues for our customers, including ensuring that users have easy access to the latest firmware installed on their Amcrest camera (https://amcrest.com/firmware).