AN INTIMATE LEAK

The true story that inspired the case:

In the autumn of 2020, click workers in Venezuela posted a series of images to online forums they used to discuss their work. In one of these images, a young woman can be seen sitting on the toilet, her shorts pulled down to her mid-thigh.

The image was not taken by a person, but by a *Roomba J7* series robot vacuum cleaner. They were then sent to *Scale AI*, a startup subcontracting workers around the world to label audio, photo, and video data used to train artificial intelligence.

Today, *'data labellers'* are often low-paid contract workers in the developing world who help power much of what we take for granted as *'automated'* online. Among other tasks, they keep the worst of the Internet out of our social media feeds by manually categorising and flagging posts, they improve voice recognition software by transcribing low-quality audio, and help robot vacuums recognise objects in their environments by tagging photos and videos.

Read more about this story:

A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?
—MIT Technology review (December 2022)

The fictional case you investigated was inspired by the true story above. This story is neither *'the Solution'* of the Investigation exercise, nor *'the Truth'*. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn't invalidate or correct your fictional work.

MY HOME STOLE MY FACE!

The true story that inspired the case:

One day, a mother from Arizona received a phone call from an unknown number and answered, worrying it could be her 15-year-old daughter, who was away on a skiing trip, trying to reach her.

On the phone, she heard her daughter's voice, crying and sobbing, saying: *'Mum, these bad men have me. Help me, help me.'* The attacker demanded a ransom in exchange for the girl's safe release.

The mother was actually deceived by what appeared to be an AI reproduction of her daughter's voice. Fortunately, she was able to confirm her daughter was safe in time to avoid falling into the trap.

Read more about this story:

Mom warns of hoax using AI to clone daughter's voice – ABC News (April 2023)

The fictional case you investigated was inspired by the true story above. This story is neither *'the Solution'* of the Investigation exercise, nor *'the Truth'*. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn't invalidate or correct your fictional work.

MYSTERY KILLING

The true story that inspired the case:

Two researchers reported vulnerabilities in *Medtronic*'s *MiniMed* insulin pump devices: an attacker could remotely target these pumps to withhold insulin from patients or trigger a potentially lethal overdose.

As neither the company nor the regulators planned to fix or replace the devices, the researchers decided to prove their point by building a '*killer app*' capable of taking control of users' insulin intake.

By default, the affected *MiniMed* models beep every time they dispense insulin, which might alert a patient to rogue pump activity. But this type of attack could happen relatively quickly, before a patient fully understands what's going on. And some patients prefer to disable the beeps anyway!

Medtronic has had similar cybersecurity issues with remotes and external programmers on other implanted medical devices, including certain models of its pacemakers.

Read more about this story:

These Hackers Made an App That Kills to Prove a Point – Wired (July 2019)

The fictional case you investigated was inspired by the true story above. This story is neither '*the Solution*' of the Investigation exercise, nor '*the Truth*'. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn't invalidate or correct your fictional work.

STEALTH INVASION

The true story that inspired the case:

A couple from Wisconsin was attacked by a hacker who managed to access their smart-home devices and terrorised them for 24 hours by cranking up their heat (their *Google Nest* smart thermostat was set to 32°C), playing '*vulgar music*' and speaking to them through a camera.

It appears that the wireless Internet system was compromised, enabling the hacker to gain access to the couple's smart-home devices. A couple in Houston reported a similar experience last year, saying a hacker announced through their *Nest* smart camera: '*I'm going to kidnap your baby. I'm in your baby's room.*'

Read more about this story:

Wisconsin couple describe the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen – Business Insider (September 2019)

The fictional case you investigated was inspired by the true story above. This story is neither '*the Solution*' of the Investigation exercise, nor '*the Truth*'. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn't invalidate or correct your fictional work.

HOME BETRAYAL

The true story that inspired the case:

Chetu, a Florida-headquartered company, fired a Netherlands-based remote worker who refused to keep his webcam on all day. The employee was instructed to take part in a virtual training period called a ‘*Corrective Action Program*’.

During the training period, he was required to remain logged on for the entire workday with screen sharing turned on and his webcam activated. He refused, stating that he felt uncomfortable and that this was an invasion of his privacy.

Eventually, the court ruled in his favour, citing Article 8 of the European Convention on Human Rights (ECHR), which grants citizens the ‘*right to respect for private and family life*’. The company was ordered to pay €75,000 in compensation.

Read more about this story:

Subjecting workers to webcam monitoring violates privacy, Dutch court rules – The Verge (October 2022)

The fictional case you investigated was inspired by the true story above. This story is neither ‘*the Solution*’ of the Investigation exercise, nor ‘*the Truth*’. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn’t invalidate or correct your fictional work.

UNEXPECTED WITNESSES

The true story that inspired the case:

Ross Compton, a 59-year-old man from Ohio in a poor health condition, was found guilty of arson and insurance fraud after data from his pacemaker was investigated and used against him in court.

While his house was burning down, he packed a bag of clothes, his computer, the charger for his health device, and broke a window to escape the fire. However, the data from his pacemaker, which the police were granted a warrant to access, provided evidence that contradicted his account of events. Indeed, his heart rate recorded before, during, and after the fire indicated that he was not in a state of rush or panic when he gathered his belongings.

Another interesting case example involving a smart device:
Richard Dabate, a 46-year-old man from Connecticut, was convicted in the murder of his wife and sentenced to 65 years in prison. The victim’s *FitBit* data showed inconsistent evidence of her movements after her alleged murder took place, not matching up to Dabate’s version of events.

Read more about this story:

Your Own Pacemaker Can Now Testify Against You In Court – Wired (July 2017)

The fictional case you investigated was inspired by the true story above. This story is neither ‘*the Solution*’ of the Investigation exercise, nor ‘*the Truth*’. The scenarios you built could have happened as well, probably. This story, if different from what you imagined, doesn’t invalidate or correct your fictional work.