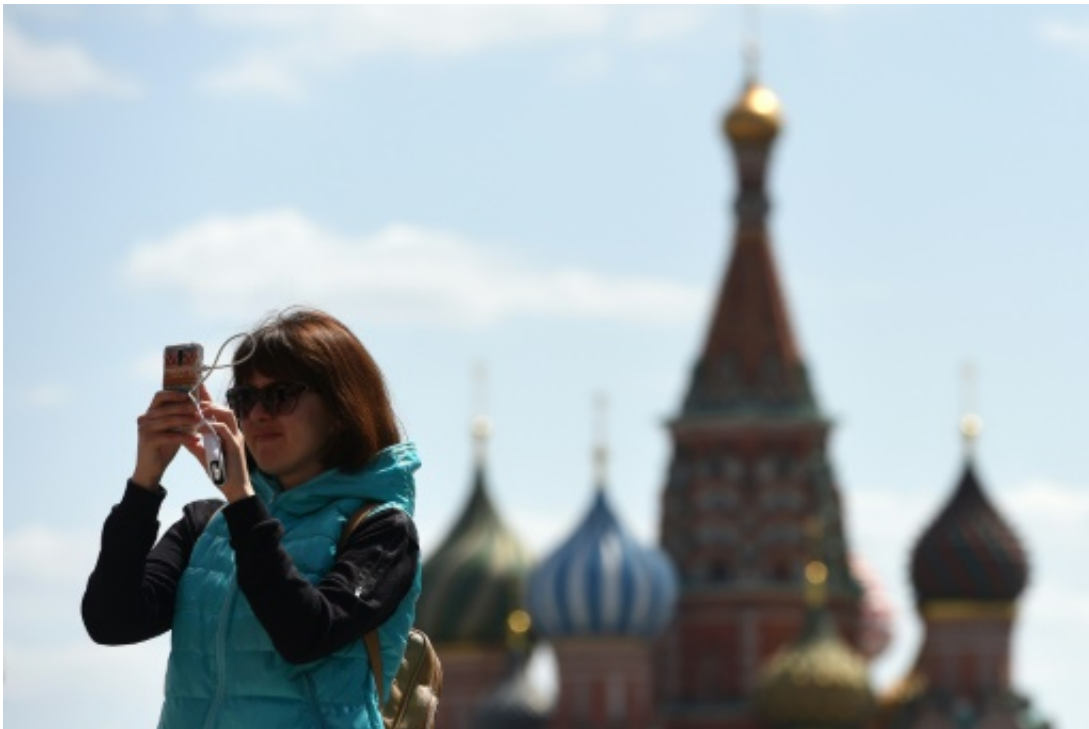


Russian hi-tech spy devices under attack over privacy fears

June 5 2016, by Germain Moyon



Russian authorities and members of the public have lashed out at recent inventions such as a phone call interception system and a face recognition app as breached of law or infringement of privacy

New Russian technologies, including phonecall interception and a facial recognition app, have stirred a fierce debate about privacy and data monitoring.

Infowatch, a Moscow-based IT security company managed by businesswoman Natalya Kasperskaya, found itself in hot water last month after it revealed it had invented a system that companies can use to intercept employees' mobile phone conversations.

Companies outside Russia have also devised call interception software, and Infowatch already markets products that monitor employees' e-mails, USB keys and printers.

But Kasperskaya says she was taken aback by the storm that surrounded the mobile phone innovation.

"We weren't expecting this. For us it was only another channel of communication," Kasperskaya told AFP in an interview.

The Russian authorities and members of the public lashed the invention as a breach of law or infringement of privacy.

Infowatch traces its origins back to 1997, when Kasperskaya and her then-husband, now divorced, Eugene Kaspersky co-founded the Kaspersky Lab security software company, which has gone on to global success.

The goal behind phonecall interception, Kasperskaya said, is to provide large businesses with a tool to prevent information leaks, including companies whose success depends on protecting corporate secrets.

Communications minister Nikolai Nikiforov said a court ruling was needed to get permission to tap phones.

The speaker of Russia's lower house of parliament, Sergei Naryshkin, said he feared such technologies could be used to malicious ends.

Facing objections from the authorities, the company has refrained from designing a voice recognition system, even though there is demand from sensitive sectors including banking, the oil industry and large public companies.



The metro in Moscow has high-speed wireless Internet, allowing commuters to use phones and computers in the trains

Monitoring of communications by private corporations touches a nerve in a country where the shadowy KGB security service once monitored dissidents and where the state is keen to retain its grip on citizens' personal data.

The KGB's post-Soviet successor, the FSB, has long used a sophisticated

system called SORM to carry out surveillance communications by telephone or on the Internet.

The revelations of whistleblower Edward Snowden showed that the US National Security Agency also carries out surveillance on a mass scale.

Human rights advocacy group Agora has said that nine million Russians, including opposition figures and political activists, have come under state surveillance since 2007.

Their mobiles have been taped, their e-mails read and their movements tracked by what Agora calls a "political policing instrument."

Infowatch has tried to assuage concerns, insisting its new system is still at a preliminary stage.

The company said that only a restricted number of telephone lines will be targeted and monitored with the employee's consent.

The monitoring is done by software that picks out key words from the phone conversations, it said.

"We have to prove that our system does not constitute phone tapping. We would by no means release on the market a system that does not respect the law," Kasperskaya said.

In any case, Kasperskaya observed, new technologies are nudging us toward a world where there are "no secrets."



A human rights advocacy group Agora has said nine million Russians including opposition figures and political activists have come under state surveillance since 2007

Finding faces

Another debate has been stirred by a new Russian smartphone app known as FindFace.

It allows users to photograph strangers on the street and identify their pages on social network site VK, Russia's equivalent of Facebook, which hosts 350 million accounts.

The app has had staggering success, with a million downloads since it was made available in February.

In half a second, the app can peruse a database of 300 million pictures and match one to a stranger's photograph, said one of the creators, 26-year-old Artyom Kukharenko, who co-founded Moscow's NTechLaB.

But in its first few weeks, the app has already brewed controversy.

Some users used it to identify the VK page of a porn actress and bombarded her with threatening messages.

On the other hand, police caught arsonists who set fire to a Saint Petersburg construction site after identifying their images on security camera footage using FindFace.

"This is a demonstration of our technology," Kukharenko told AFP, adding that his app had garnered interest from companies throughout the globe.

"The real use of the algorithm will be for security services, banks, distributors and for leisure activities," as well as for dating services and those who wish to meet strangers they saw on the street or even someone who just looks similar, he said.

IT security specialist Mikhail Yemelyannikov told AFP that FindFace does not violate any existing legislation because the social media pages it trawls contain pictures with unrestricted access.

"The problems start later: what will the result be used for?" he said.
"Legislation will never evolve as fast as technology."

© 2016 AFP

Citation: Russian hi-tech spy devices under attack over privacy fears (2016, June 5) retrieved 9 April 2024 from <https://phys.org/news/2016-06-russian-hi-tech-spy-devices-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.