INFOWATCH®
WE WORK TO PROTECT

Ph.: +7 (495) 22-900-22
+7 (499) 37-251-74

Russia, 121357, Moscow,
29/134, floor 7, Vereyskaya street
BC "Vereyskaya Plaza"

www.infowatch.ru

Apple against the FBI: whose side Russian experts

The massacre of the people in San Bernardino Western society divided into two camps. One turned out to be opponents of spying and disclosure of personal data, in the second - the maximum assistance to proponents of the secret services. "Apple of discord» - iPhone one of the terrorists, which the FBI through scandals and lawsuits trying to find important data. It turned out that the security forces support a significant part of society, and many people in different countries are willing to exchange freedom of information on personal safety. The Digital Report publication decided to find out from the Russian experts, whether it is worthy of sharing.

Group CEO InfoWatch Natalya Kaspersky:

Should there be a legitimate opportunity for the government to gain access to personal data on smartphones, computers citizens? Since we know that there is a kind of state, which has the access and without the desire of our citizens, and without the desire of our country, it is likely it would be logical that our state also had the opportunity, for example, with a good view to combating terrorism and not only that one foreign country

Once you buy a smartphone (. Internet access, a crank yourself an account in social networks, Instagramme, messenger, make a search query, etc.), then any of your actions automatically:

a) monitored by this network, messenger, search engine, etc.,
b) written to permanent storage,
c) it becomes the property of the special services of a foreign state.

No right to privacy of the person who uses modern communications technology, no. This is written in the license agreements of software products, and is not recorded, but done after the fact. Therefore, neither of which privacy is not the issue. The question should be put this way -

Ph.: +7 (495) 22-900-22
+7 (499) 37-251-74

Russia, 121357, Moscow,
29/134, floor 7, Vereyskaya street
BC "Vereyskaya Plaza"

www.infowatch.ru

whether it is necessary to disclose their activities in the network and even its own intelligence agencies? In fact, if special services want information about a face, they did, of course, receive, including, by obtaining access to electronic communications. Therefore, honest citizens to lose here, in general, nothing. And about fraudulent it is clear - they have to catch.

Incidentally, I once talked with a former detective. He said that the crime detection rate of car theft in recent years has grown at the expense of electronic communications -. Results cameras views, traffic analysis, etc. So it's a chance to win some kind of crimes - such as terrorism - by monitoring systems or simple monitoring devices.

Kirill Bragin, head of the Agency of internet technologies GoodSellUs:

The state has a legitimate opportunity to get access to your personal information and correspondence. According to the court you can withdraw the personal computer or mobile phone and have access to it. The same goes for tracking location via a mobile device and the other "a terrible thing", which simply do not think or do not know. That is the question "Do? May" is not worth it.
The government always intervenes in the personal lives of every citizen, whether he wants to or not, and always restricts the freedom of the citizens with a view to the safety of citizens and the integrity of the state. The same goals are censorship and propaganda - the creation of a single public opinion, which will survive the crises, terrorist attacks and other difficult times.

Victims of terrorist attacks less than the victims of accidents or domestic murders, but victims of terror - terror - getting. Fear pervades all strata of society, and now scared to use the metro, and tomorrow go out.

Is the absence of fear violation of civil liberties? I think yes. Will there be another state to take such steps? Definitely.

Nikolay Kalmykov, director of the Expert-Analytical Center, Russian Academy of National Economy and Public Administration under the President of Russian Federation (RANHiGS)

Always important is the right balance. Speaking of that security should not have access to the personal data of potential offenders, many somehow emanate from such a position that no one allegedly did not have real access to these data. But what about the companies themselves, on whose servers the data services work? What an illusion that they can not view or use this information in their competition, competitive intelligence? And if we talk about the situation in different countries - we know not only a couple of precedents ostentatious refusal to give data

Ph.: +7 (495) 22-900-22
+7 (499) 37-251-74

Russia, 121357, Moscow,
29/134, floor 7, Vereyskaya street
BC "Vereyskaya Plaza"

www.infowatch.ru

security services, but examples of situations in which the data were transmitted to the authorities, including in countries such as the United States.

Again, what is privacy when communicating on public resources? How it privately?
In any case, the citizen must be at least warned that his correspondence and data can be anywhere on-demand security services - it is the first necessary step. As for the decisions about whether or not to give such access - is necessary to proceed from reality, and they are such that this practice exists. Together with this, as clearly necessary to regulate such requests and provide maximum protection for both the individuals from abuse and data that can be obtained in accordance with such requests.

Mikhail Salkin, director of the Moscow Human Rights Center

This opportunity should not be. Taking into account the high level of corruption in law enforcement access to such information and the information itself immediately become interested in Commercial and raider attacks, it can be used to the detriment of citizens.

Moreover, it is inadmissible without the decision of the court to view the correspondence of citizens. That messenger is the main object of interest of law enforcement and intelligence agencies.
Rigorous screening procedures at airports of airline safety rules clear example of such restrictions

Vladimir Lebedev, Director of Business Development Stack Group

In my opinion, it should be a balance between the constitutional rights of a citizen and the right to carry out operational activities to curb illegal activities. In today's world of constant access to information and means of communication available today almost all the citizens who have access to the Internet should be mechanisms to prevent the spread of illegal information. However, the use of total control over the personal data must be adequate mechanisms to be compared with a real opportunity to stop the illegal actions.

Rigorous screening procedures at airports of airline safety rules clear example of such a restriction, but a total legal access to personal data, correspondence - it is a violation of the right to privacy, personal and family secrets. Adequate if such security measures the real effect of such access? In my view, in special cases, in the course of an investigation in a particular case - of course, totally - no.

Source