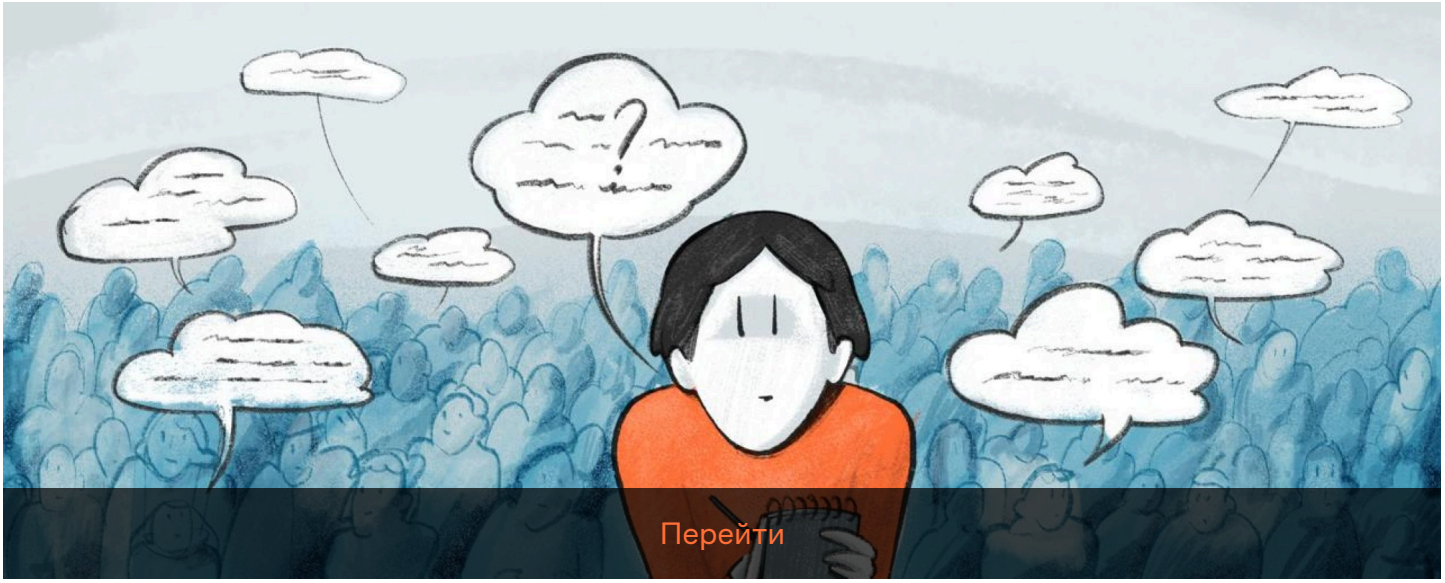

26.07.2024

Guide on General Safety for Foreign researchers that plan to work with Russian participants

How safe is it to conduct social surveys or have an interview if your participant is in Russia? What if you were labeled as foreign agents or part of an «undesirable» organisation? In this guide, we have collected the main principles of digital and general safety that will be useful in such cases.

If you plan to organize/participate in such research, and you would like to understand your risks, contact us via Telegram bot or email at data@ovdinfo.org.

ASSESSMENT AND MINIMISATION OF RISKS

Is it ethical, or even possible to conduct research in Russia for the foreign scholars? And if it is, what should they keep in mind to keep the process safe for all participants?

The Russian state often designates foreign people and organisations with negative statuses which complicate their cooperation with Russian citizents. It also affects people who interact with them. Many human rights organisations, independent media and people involved in human rights protection, journalism, and activism are recognized as «foreign agents», including OVD-Info. This also applies to researchers and universities: for example, the Central European University and Toronto University have been designated as undesirable organizations. «Undesirable» and «extremist» organisations, which entail even greater restrictions on rights and freedoms.

Foreign agents. As for foreign agents, this status is formally assigned to those people and organisations which are engaged in «political activities» and at the same time «receive foreign funding» (you can read more about this in the material of the Media Rights Protection Fund). If you were designated as «foreign agent» and plan to involve Russians in your research (for example, to involve them as respondents, research colleagues, contractors or assistants in distributing research results, or vice versa, to participate in their research), it is important to think through your strategy in advance. If you have been labeled as a «foreign agent» and you plan to send payment for participation in the study, the people you work with are also in danger of being labeled as a «foreign agent». If you wish for those people or organizations to avoid acquiring this status, it's advisable to channel funding through third parties and organisations or in cryptocurrency (details below).

If you do not pay participants money for participating in the research, according to the law such a cooperation is safe. If that individual is not a public person (and is not going to become one) and have not attracted the attention of law enforcement before, the risks are minimal. At the same time, you need to be prepared for the fact that if your participation is public, then the person will «get on the radar» of law

enforcement officers, which will increase the risks of being a «foreign agent» and other risks for them. The same applies to reposts of materials created by «foreign agents», subscriptions and donations: there is no responsibility, but we do not know how it will actually happen. So, the journalists Olga Churakova and Sonya Groisman formally received the «foreign agent status» for the reposts of other «foreign agents», but most likely the real reason was their own work.

If you want to be cautious, encourage research participants to not discuss your collaboration publicly and on social media. It is also better if you refrain from mentioning personal details in the text. You can always ask the people you collaborate with if they allow you to publicly mention their name or include any of the documents — you shoud should accommodate their request.

Undesirable and extremist organisations. If you are labeled undesirable or extremist organization — your work is actually prohibited in Russia, and collaboration with you can lead to administrative or criminal liability for Russian citizents. If such cases you can still conduct your research, but we do not recommend publicly discussing your collaboration. Clarify safety protocols with participants of your research and strictly adhere to them. It's advisable to provide anonymity for the person you collaborate with.

If you are working with a Russian citizen currently located in the European Union or another safe country with no immediate risk of detention or imprisonment, you should still exercise caution. For example, Russians could potentially face severe financial penalties in the form of hefty fines. For more information on interactions with «foreign agents,» «undesirable», and «extremist» organisations, please refer to our information cards.

HOW TO MAKE IT HARDER TO TRACE YOU: BASIC DIGITAL SECURITY

To prevent your personal data from being leaked to Russian Security Forces, you and the respondent you reach out to should follow certain cybersecurity rules. OVD-Info has prepared a guide on digital security for respondents (In Russian). If you're recruiting Russian citizens for your study, you can advise them on following it and, in case they have questions, contact OVD-Info for assistance.

If you plan to propose an online interview, we recommend using Telegram, Signal, WhatsApp, Google Meet, or other similar messengers. Avoid providing any sensitive information on VK and Yandex platforms or during phone calls with a Russian SIM-card. Hide phone numbers in messengers (available in Telegram and Signal), and enable call relay settings (Telegram: «P2P calls — never»; in Signal and WhatsApp, it is simply called «relay calls»). If you happen to connect with a hostile party with strong technical skills, having VPN and call relay enabled will prevent them from determining your location. Additionally, set auto-delete timers on especially sensitive chats.

If you need to make a mobile phone call, remember that your conversation will not be private, as it will pass through cell tower transmission. Do not discuss anything 'dangerous' during such calls.

Avoid using Russian browsers, as they can trace all your actions on the Internet. Encourage your participants to not use Russian programs that have wide access to your system, such as Alisa. You don't have to switch completely to inconvenient browsers like Tor, simply replace Yandex with Chrome or Firefox.

Basics of secure data storage, transfer, and deletion

1. To ensure secure data and files storage, all of your cloud accounts should be protected with a complex password and two-factor authentication. Devices and external disks should be encrypted. If encrypting flash drives and other storage devices is too difficult, try to store files only in the cloud using a non-Russian service and only work with the files there.

2. If you are particularly worried about certain files or folders, they can be encrypted separately before being loaded to the cloud. There exist several programs which do not allow decrypting certain files without a password (if this sounds too complicated for you, please watch this 5-minute video by Teplitsa — a public educational project aimed to develop cooperation between non-profit sector and IT-specialists).

3. Share files and documents by giving access to them in the cloud. Only allow access by mail, as sharing a file by link makes your document or file publicly available.

4. Information that enters your computer or external driver never disappears without a trace; it can be recovered if the driver wasn't encrypted before files ended up there. This isn't done to harm you but to ensure modern disks are resistant to deterioration. If you have files and documents that must never be found on your device, do not delete them in the usual way. Instead, use the Eraser program (for Windows). This program will overwrite the necessary files with random data, making them impossible to restore. MacOS is more complex, and it's hard to find a program for such rewriting. But once again, storing and working with data in the cloud will eliminate these problems.

If you are a specialist in digital and legal security, ethics of research during wartime, or you have experience conducting research in present-day Russia and find inaccuracies in this text, please contact us at data@ovdinfo.org.

ETHNICAL GUIDELINES SUGGESTIONS

Most ethical guidelines are relevant to any research field, but there are some specific considerations for Russia. Firstly, in Russia there is no centralised ethics committee that approves research designs, and secondly, war and repression introduce new challenges. Above, we have outlined guidelines and principles that we use ourselves.

1 Integrity Principle.

a. Do No Harm (non-maleficence). The research should not be directed against specific individuals, groups of people, or society as a whole. However, research can be aimed at addressing a social problem; in this case, the risks to individuals and groups must be justified, minimised, and balanced by the public benefit (see point 2).

b. Less is more. The gathering of respondents' data should be justified; prior to gathering the data, all existing publications and data sets should be considered. If and when respondent data is gathered, it should be processed and utilised accordingly.

c. Compliance and excellence standards. The research should be carried out in accordance with international methodological standards and as thoroughly as the circumstances and capabilities of the researchers allow.

d. Transparency. Whenever possible, researchers should make the data collection and analysis process transparent, and the results and data should be made public.

e. Sustainability. Researchers should not, through their actions, block access to respondents for other researchers or lead to a loss of trust in research as a whole.

f. Reflexivity. Researchers should recognize the impossibility of complete research neutrality and make every effort to explicitly identify and reflect on their own political and civic positions. Discussion within the research team and consideration of these aspects when planning, conducting, and presenting research results are mandatory.

2 Principle of utility. The research must be of benefit to the group of people being studied or to society as a whole.

a. Utility refers to the protection and support of human rights and freedoms, including the right to access information, the restoration of legal, social and historical justice, the improvement of the quality of life and similar objectives.

b. Gaze. Social research is not neutral and it is focused on people or communities in one way or another. For this reason researchers must, whenever possible, give voice to the most vulnerable, marginalised, poorly represented people and communities in the public discourse.

3 Rights Respect. Research as a whole must respect and uphold the rights, freedoms and human dignity of respondents.

3. 1 Failure to respect a respondent's rights can take many forms, including:

3. 1. 1 Direct harm to the respondent's health, including psychological harm (through retraumatization in particular)

3. 1. 2Disclosure or leakage of personal and sensitive data of the respondents, including data on participation in the research, resulting in:

3. 1. 2. 1Harm to the respondent's health by third parties

3. 1. 2. 2 Being politically persecuted by Russian political regime (initiation or intensification of repressions)

3. 1. 2. 3 Loss of migration, social and other rights and privileges (both in Russia and abroad

3. 1. 2. 4 Loss of status, employment, professional or personal reputation, capital, deterioration of living conditions

3. 1. 2. 5 Acquisition of negative, stigmatising status or otherwise deterioration of social status

3. 2 To avoid causing harm to respondents and themselves, researchers **must**:

3. 2. 1 Where possible, obtain and document (in writing or by recording) respondent's informed consent for data collection. Consent must also cover the specific method of collection (audio/video recording, transcription by third parties, etc.).

3. 2. 2 Only use safe locations for offline meetings, secure communication channels and storage methods, and ensure safe handling and analysis of information. Do not store personal data of respondents in the same repository

as sensitive collected data. Separate respondents' data from the personal data of the researcher. Use pseudonyms and other data protection measures for respondents.

3. 2. 3 Do not transfer respondents' data to third parties. If a contractor requiring access to the data (such as an interviewer, transcriber, editor, etc.) is engaged for the interview, the data must be provided in the minimum possible set while maintaining anonymity (i.e., without revealing the respondent’s personal data). Contacts can be shared with third parties only with the participant’s permission. The responsibility for verifying the contractor’s reliability rests entirely with the researchers.

3. 2. 4 Publish respondent data exclusively in an anonymized and aggregated form. All publicly accessible data, including quotes, photographs, artefacts, etc., must be stripped of personal data or any information that could easily identify the respondent (such as involvement in a high-profile media story, living in a small community, having a rare illness, etc.).

3. 2. 5 Take care of their own digital, physical safety, and psychological readiness to work with respondents from unfree societies, especially those who are vulnerable or have experienced violence. For methods of self-care, see above.

3. 3In cases where participation in the research involves risks described in point 3a, researchers must inform respondents in advance (for respondents under 14 years old, their parents or guardians).

3. 4 If harm is caused to respondents, researchers and their affiliated institutions bear full moral responsibility for it.

4 The equivalence of transparency in your research and the future accessibility of data for other researchers should be considered. In some situations, informing respondents that you are conducting research may lead to a loss of trust and the inability to collect data—for example, if you are conducting ethnographic analysis in Russian state structures. In this case, researchers need to weigh the following aspects:

4.1 **The importance of informed consent:** Where possible, and always in cases of interviewing, surveying, or collecting personal data both offline and online, the researcher must create a safe space for the respondent and inform them (for respondents under 14 years old, their parents or guardians):

4.1.1 About the purpose of the research and the reasons for recruiting this particular respondent.

4.1.2 About the topics of interview or survey questions and the possibility to refuse to answer any question, end the conversation, or reschedule it to another time, format, or location.

4.1.3 About the option to withdraw from the study at any stage up to the publication.

4.1.4 About any recording of the conversation (photo, video, audio, or written) if it is being conducted.

4.1.5 About how the collected data will be used.

4.2 **Access to data**: When the public benefit of conducting research is particularly high and data availability in Russia is low, it is permissible to conduct participant observation, both online and offline, without prior approval, especially if obtaining such approval poses risks to the researcher or respondents. However, collecting personal or sensitive data is strictly prohibited in this case.

5 **Decision on prioritising transparency or data access:** The decision on whether to prioritise transparency or access to data is made on a case-by-case basis, and researchers and their affiliated organisations bear responsibility for the consequences. Researchers should, where possible, discuss such decisions collectively and provide justifications for them.

MAKING YOURSELF HARDER TO IDENTIFY: BASIC DIGITAL SECURITY

1. Every account you use, whether personal or work-related, must be secured, even if it seems insignificant. Your communications and files must be protected from law enforcement agencies, and your social media and government service accounts from malicious actors.

2. Passwords for all your accounts should be unique and long. Use a password manager to generate random 16-character passwords and change them for all the accounts you use. It might be helpful to first make a list of all your accounts: email, social media, Telegram, Gosuslugi (Russian app for public services), work services, even insignificant and unused accounts. You don't need to memorise these passwords; you can always copy them from the password manager. We recommend Bitwarden.

3. You generally only need to memorise two passwords: one for your password manager and one for your computer. Since remembering 16 random characters is very difficult, you can use passphrases instead.

4. Every account should have two-factor authentication enabled, which you can activate in the account settings. SMS is not reliable, so instead, or in addition, use an authentication app. We recommend 2FAS; it's secure and easy to use. Try linking one account to it, and you'll see how simple it is. The only exceptions are messaging apps like Telegram and WhatsApp, where the first step is a verification code, and the second is a password (in Telegram) or a PIN code (in WhatsApp and Signal).

5 Hide phone numbers in messaging apps (this feature is available in Telegram and Signal), and enable call relaying in the settings (disable P2P calls in Telegram; in Signal enable option «Always Relay Calls», and in WhatsApp, turn on the setting «Protect IP address in calls»). If a malicious actor calls you, having a VPN and call relaying enabled will help protect your location from being easily traced. Additionally, set auto-delete timers for particularly sensitive chats.

6 Try to minimise the use of accounts on Russian services for research purposes. If you've connected with a respondent on VK, invite them to communicate further on Signal or Telegram. Keep your Yandex account for deliveries and taxi services, and for communication and document storage, opt for Google instead.

7 If you need to make a call to a mobile phone, remember that it cannot be completely private because it goes through cellular towers. Avoid discussing anything sensitive for you or the informant during such calls. If you simply need to hide your number from the person you're calling, use any IP telephony service or Skype.

8 After setting up your accounts, it’s crucial to protect your devices from data interception when connected to the internet and from situations where your computer or phone may fall into the hands of malicious actors:

8.1 Keep everything updated: your phone and computer systems, as well as programs and applications. Hackers, including those working with governments, are constantly looking for new ways to breach security, while developers continually strive to protect their products. Each update brings new security measures, so remember to install them regularly.

8.2 A VPN encrypts the data you send while you're online, and without a VPN, your internet provider can see much of what you do online. Using VPNs in Russia is still legal, it is only illegal to post information about them publicly. Try to keep your VPN turned on at all times; we recommend services from the vpnlove.me list

8.3 Set a short screen lock time on your computer and replace any simple passwords with a passphrase. On your phone, also set a short screen lock time and an unlock code with no less than a 6-digits. In many applications, you can additionally set PIN codes both on your phone and on your computer, for example, Telegram and Signal.

8.4 Check if your devices contain Russian certificates that can be used to intercept and decrypt what you do online. There are instructions for macOS here, and on the same page in Notion you can find instructions for any phone or computer system. If you need a certificate from the Ministry of Digital Development (for example, to use an electronic digital signature), then it is better to have a separate device for such manipulations (or a separate browser, but without a certificate not everything you need may work in the system).

8.5 Enable encryption for your device. Modern phones usually have encryption enabled by default, while computers require special programs. macOS has built-in FileVault, Windows 10 and 11 Pro have BitLocker, Linux has LUKS, and Windows Home versions have VeraCrypt. Encryption is not easy, so check out the step-by-step instructions here.

8.6 Enable antivirus software on your computer. The built-in programs are no worse than paid ones, so you can safely enable Firewall in macOS or Windows Defender. If you want to install an additional antivirus program, take a look at McAfee, Norton, Avast and Bitdefender. Under no circumstances use Russian antivirus programs such as Kaspersky and Dr. Web.

8.7 Do not use Russian browsers — they can track your every action online. It is also worth getting rid of Russian programs that have wide access to your system, such as Alice. You don't have to constantly work in inconvenient browsers like Tor; you can easily replace Yandex with Chrome or Firefox.

WORKING WITH MONEY

During the research, you may need to work with money: for example, if your research is funded by a foundation or you need to transfer payment for participation in the research to your respondents. There are several ways to receive funding from foreign organisations, as well as from organisations and people with a negative status in Russia («foreign agent», «undesirable», «extremist»), which can be called relatively safe for the recipient. Here they are: cash payment, cryptocurrency payment (but not any!), and through a third-party person or an organisation that is located in Russia and is not under the radar of security forces.

Cash payment is the safest option, but for this the recipient needs to go abroad (for example, to Georgia); if we are talking about paid participation in a study, this method is not possible. In addition, there are different restrictions on the import and export of currency in different countries. Another relatively reliable alternative is to pay for the services of researchers and respondents located in Russia through Russian legal entities (for example, commercial ones), or from the bank cards of individuals. However, in this case, the problem shifts further: how to transfer money to the accounts of these extra financial «layers» if you need to do it from abroad?

If, for some reason, other payment methods are unavailable, you can try transferring money in cryptocurrency. As of June 2024, cryptocurrency has a «grey» legal status in Russia: officially, you cannot buy goods or services with crypto, but investing in cryptocurrency exchanges is permitted (see Federal Law No. 259-FZ of July 31, 2020). Therefore, purchasing rubles with your cryptocurrency assets is currently legal in Russia; this may change in the future.

It is important to remember that the purchase, for example, of bitcoin, by the sender, transfer to the recipient's wallet and subsequent purchase of rubles by the recipient are not anonymous actions themselves: the source and destination of the payment can be tracked. The FSB has already done this (see the high treason criminal case for donating to the Armed Forces of Ukraine). In order to anonymize your cryptocurrency operations, you need to use a completely anonymous currency; at the moment we are aware of only one currency of this kind, and that is Monero.

Here is the algorithm for anonymously obtaining cryptocurrency «for dummies»:

1. Set up any convenient «non-anonymous» cryptocurrency wallet for you and the sender, such as Trustee Wallet. Registration should not require your passport details; if it requires an email, it is better to use a specially created email account.

2. Ask the sender to buy the cryptocurrency that is convenient for you (for example, USDC ERC20, which is tied to the dollar exchange rate) using any online platform. For Russian cards, you can find a seller, for example, on the BestChange.ru exchange.

3. 3. Receive the payment in cryptocurrency to your wallet (important: if the currency operates on the Ethereum network, you will also need to buy some «ether» before receiving the transfer).

4. 4. Install the Monero GUI Wallet program from the official Monero website. During installation, select the «Simple mode bootstrap» and create a Monero wallet — it will be completely anonymous.

5. 5. In your «non-anonymous» wallet, buy Monero and transfer it to your anonymous wallet.

6. 6. From your Monero wallet, withdraw the money to your bank card or to an offline ATM again through BestChange.ru.

If you have attracted the attention of law enforcement

For example, if you are researching «extremists», and now they also want to label you as an extremist, or if you participated in a study of an «undesirable organisation.»

Interrogation

If you are summoned for an interrogation, you will be assigned a procedural status. This is your role in the criminal case — the procedural status determines your rights. The status is indicated in the summons. If it indicates one

status (e.g., a witness), and you arrive only to be told that the status has changed (e.g., to a suspect), demand a new summons and the presence of your lawyer. Do not agree to a lawyer appointed by the investigator.

Being a witness

On one hand, the status of witness is the most harmless compared to others. On the other hand, this status grants fewer procedural rights and can change very quickly. Remember that any word can be used against you, and after an interrogation as a witness, you can move to the status of a suspect.

As a rule, at the beginning of the interrogation, the investigator establishes your identity: you will need to provide your passport or another identity document. The investigator will ask questions to record your personal data in the Interrogation Protocol (full name, registration address, place of work, etc.). You need to answer these questions.

You must be informed about the reason and the capacity in which you are summoned. The investigator is obliged to explain your rights as a witness according to Article 56 of the Criminal Procedure Code of the Russian Federation. After that, you will need to sign the corresponding part of the protocol. Following this, questions regarding the substance of the case will begin. The main thing to remember is that you are not obliged to testify against yourself (Article 51 of the Constitution).

Try to answer briefly, thoughtfully, and calmly. Only answer the question that was asked.

What not to do:

☒ Do not tell the investigators your life story and try to «explain everything»;

☒ Do not refuse to give testimony entirely. This carries criminal liability.

However, when answering the investigator's questions, you can, for each specific question:

☒ Forget or not know something — you can calmly respond this way (I don't remember/I don't know).

☒ Use Article 51 of the Constitution if you believe your answers could harm you.

☒ If you are asked about your political beliefs, you have the right to refuse by referring to Part 3 of Article 29 of the Constitution: «No one can be forced to express their opinions and beliefs.»

☒ You should not contradict yourself; you should not deny facts that were already established in other cases.
It is of utmost importance not to tell any lies — this will be discovered instantly and after that the interrogation process can become unpredictable. At the very least the investigator will become highly sceptical of all your following answers.

At the end of the interrogation, you are allowed to see the interrogation protocol. Read it carefully and ask to fix any issues or any inconsistencies between your original reply and the written version. If the interrogator refuses to amend the protocol, mention this fact when writing down your comments to the protocol.

In the comments, if needed, add a summary of what you actually said during the interrogation. Ask the interrogator to cross all empty lines, so that nobody would be able to add anything after the fact; however, you do not do that yourself.

In the interrogation protocol there may be an item like «I consent to being summoned to the court by SMS

message.» You can agree to that, but in general it is better to receive such notifications through regular mail.

Only sign the interrogation protocol after completing all the previous steps.

Interrogation of a suspect

Being a suspect is, of course, much more dangerous than being a witness. However, this status also offers more processual rights.

The interrogation of a suspect or of an accused must be conducted in the presence of the lawyer. It is of utmost importance to attend such interrogation with your personal lawyer or the one provided by a human rights organisation. Never accept a lawyer that is provided by the Russian government (state-appointed lawyer) — unfortunately, such lawyers are known not to act with integrity or in the best interests of their client.

Additional rights of a **suspect:**

- You have the right to call a lawyer and be interrogated in his presence. This means that if you think you might become a suspect, you need to sign an agreement with a lawyer beforehand.
- You should be allowed at least 2 hours of private communication with your lawyer.
- You can decide not to answer the interrogator's questions. This does not result in prosecution as per part 2 of Article 46 of the Criminal Procedure Code of the Russian Federation. If you are a suspect, you have a right to interact with investigators only in presence of a lawyer.

An accused has the same rights as a suspect. In addition to that, an accused can access all the case data as soon as the preliminary investigation ends.

Search

Usually the searches are conducted around 6am. Law (part 3 Article 164 of the Criminal Procedure Code of the Russian Federation) forbids any investigative activities, including search, during the night time (from 10pm to 6 am), except for emergencies.

If the policemen come knocking at your door early in the morning, **do not open the door immediately**! Start by asking them about the reason for the visit. If they say that they have come to conduct a search — ask them to show the search warrant to you through the peephole. After that, say that you are calling your lawyer now and that you will open the door as soon as the lawyer arrives. Please keep in mind that the search warrant must contain the case number and your address — if those are not there, you are not required to open the door. However, there is always a risk that they will break the door and get in with force.

Make sure to inform your friends and family about this situation.

You have the right to make only one phone call — this means you need to learn by heart the phone number of your lawyer or of a close friend you can pass the information to and who can find the lawyer for you.

It is important to know that recently police started to arrive to a search with a state-appointed lawyer in tow. You need to insist on your personal lawyer, since state-appointed lawyers are known to act in the interest of police and interrogators.

Your rights during a search:

- To have a lawyer present;
- To be present yourself during the search;
- To observe the actions of those conducting the search;
- To not testify against yourself or your loved ones: this right is given to you by Article 51 of Constitution of Russian Federation (the right to not self-incriminate);
- Under no circumstances should you give the investigator the passwords to your computers, mobile devices, email services, messengers, or social networks: this right is also given to you by Article 51 of the Constitution of the Russian Federation;
- To demand non-disclosure of details of your private life, personal and family secrets discovered during the search;
- To demand the presentation of items that they intend to seize and their inclusion in the report;
- To make notes in the report;
- To receive a copy of the search report.

Remember that you have the right to read the search warrant; if you cannot take a photo of it, you have the right to make a copy by hand.

Based on the search results, a report is drawn up. Carefully read the report and indicate all possible violations/abuses by the investigators. The report must include:

- Date and time of the beginning and end of the search.
- Names of all persons present during the search.
- A description of the course of the search.
- A list of confiscated items — request that the items be described in as much detail as possible (not a «box of things, ” but a list of models and numbers of electronic devices).
- All empty fields must be crossed out.

Indicate ALL comments. Especially if during the search they «found» something that you did not have. You can take as long as you need to write down all the comments. If the comments are attached on a separate sheet, indicate this in the report and briefly describe it.

Be prepared to be detained after the search. Pack essentials, inform your friends/relatives and your lawyer where you are being taken.

Tips During a Search

- Prepare a pen and a notebook/diary, where you will record everything.
- If a lawyer cannot be present personally—keep in touch with the lawyer by phone. **It must be an «empty» phone which does not contain important information, because at some point it may be confiscated by investigators.**
- If a lawyer is not allowed—inform all participants of the search about it and later add this information to the report.
- Do not try to prevent the investigation team from entering. This could be grounds for initiation of a criminal case against you.
- Before the start of the search, the investigator must introduce himself, state which criminal case the investigation is related to, show the rulings and clarify your rights.
- Before the search, you will be asked to voluntarily hand over prohibited items and/or information necessary for the investigator. You are not required to do this under Article 51 of the Constitution. You have the right to hand them over, but it is worth remembering that it will not make your fate easier—it will not be a mitigating circumstance. Therefore, think carefully before giving anything away.
- The search is carried out in the presence of two witnesses. Write down the names of the witnesses, and ask them if the addresses that they specified match the addresses of their residence.

- Try to control the actions of the investigators: if possible, demand that the search be carried out sequentially in different rooms. Write down all comments in a notebook and then include them in the report. The comments may include rudeness, disrespectful attitude to your property—if something was broken/smashed, etc. If the investigators enter a room or open a box without you, make sure to write it down.

Here (in Russian) you can find information on how to manage digital security on your devices before, after and during the search,

ACCESS TO STATE SECRETS, PRESENCE IN RESTRICTED AND HAZARDOUS SITES

For example, are you going to gather information about restricted and hazardous sites, such as the construction of Putin's palace or a military plant? Below are some safety measures you can take.

1. To search for information online, launch a VPN and then the Tor browser, precisely in that order. First, turn on the VPN to encrypt and hide your data from the Internet provider. Then, launch the Tor browser, which will provide maximum privacy when visiting the sites you need.

2. While doing such research, avoid using accounts in Russian services entirely (VK, Yandex, etc.); even if this simplifies the work, any login can de-anonymise you.

If you want to visit such a place physically:

3. When we talk about dangerous places that, in principle, are better not to visit at all, ideally, you should go without devices that can connect to the mobile network (cameras and devices for sound recording are OK).

4. If leaving your phone far from the place of the planned visit is impossible, you can use a spare one, but this is a problematic and unreliable option: if your spare and main phone are located nearby, they are identified as devices belonging to the same person. Therefore, your spare phone must be stored outside the home and work, which is not always an option. Turning off the spare phone does not solve the problem.

5. A good option could be a Faraday cage — a special phone case that does not transmit signals. You must put your phone in such a case well in advance and far away from your destination, and not open it until you get to a safer space. You can buy a Faraday cage on any marketplace, and check it by simply putting your phone inside and making a call from another one. If the cage works, it is going to be impossible to get through.

6 If you go to a place that is legal to visit, but you need to hand over the device at the entrance to a storage room (government institutions or restricted sites such as a pre-trial detention centres), you should comprehensively configure the security of your phone (this will be discussed in the following sections). A separate important setting for such situations is to **turn off control of a locked device using USB**. There are accessible instructions for this setup for Android and iOS.

7 Moreover, when going to any place where your phone might be taken into storage or confiscated, create a separate account on your phone (Apple ID or Google) so that you can log out of the main one and not worry about passwords, the two-factor authentication, and other personal information.

8 If you took photos or videos on-site, you should remove the metadata before sharing them with anyone or uploading them to the cloud. Good software options for removing metadata are ExifCleaner (for any computer), Metapho (for iOS), and EXIF Fixer (for Android).

If you are offered to participate in a study and want to understand your risks and decide whether to agree, write to us via bot or email data@ovdinfo.org.

If you are a specialist in digital and legal security, the ethics of research during wartime, or have experience in research work in current Russian conditions, and find an inaccuracy in this article, please let us know via email at data@ovdinfo.org.

To help international scholars in producing insightful and ethical research about political repressions and civil society in Russia, we at OVD-Info are happy to assist them as much as we can. If you need ethical, legal or digital guidance for yourself or you Russian collaborators and informants, or you're searching for some data, or would like

to be introduced to the Russian NGOs, human rights advocates, researchers, journalists and activists, please submit your request here.

Request assistance with your resea from OVD-Info

To help international scholars in producing insightful and ethical research ab political repressions and civil society in Russia, we at OVD-Info are happy to them as much as we can. If you need ethical, legal or digital guidance for y you Russian collaborators and informants, or you're searching for some dat would like to be introduced to the Russian NGOs, human rights advocates, researchers, journalists and activists, please submit your request here.

Name *

What is your name?