SOCIAL SCIENCE RESEARCH COUNCIL | WORKING PAPERS

DATA SECURITY IN HIGHLY VIOLENT SETTINGS

ENRIQUE DESMOND ARIAS

DRUGS, SECURITY AND DEMOCRACY PROGRAM
DSD WORKING PAPERS ON RESEARCH SECURITY: NO. 7

ABOUT THE PROGRAM

The Drugs, Security and Democracy (DSD) Program strives to create a stronger, more systematized knowledge base on drugs, security, and democracy in Latin America and the Caribbean; to build capacity—both institutional and individual—by supporting relevant research; and to encourage policy-relevant, evidence-based research that could lead to the development of alternatives to present-day drug policies. Support is provided for research across a variety of disciplines—anthropology, criminology, economics, history, international relations, journalism, legal studies, political science, public health, public policy, sociology, and other related fields—to create a network of scholars interested in developing alternative approaches to drug policy.

ABOUT THE SERIES

Over the last generation, activists, journalists, and researchers working in Latin America have increasingly faced the challenge of operating in areas affected by chronic police and non-state violence. Further, rising crime rates are leading a growing number of scholars to conduct research on high-risk topics, which involves gathering data on communities that experience conflict, writing and publishing on these difficult and sensitive issues, and developing and implementing programs to deal with the needs of communities affected by violence as well as the wider conflicts in which those communities are embedded. Despite these trends, the literature on safe practices for those working in high-risk environments remains thin. The DSD Working Papers on Research Security series seeks to address this deficit by examining a range of research security concerns, providing a framework to help those working in the region consider how they can enhance their own safety as well as the safety of their associates and research participants.

The DSD Program is funded by the Open Society Foundations. The program is a partnership between OSF, the SSRC, Universidad de los Andes in Bogotá, Colombia, and Centro de Investigación y Docencia Económicas in Mexico.

DATA SECURITY IN HIGHLY VIOLENT SETTINGS

ENRIQUE DESMOND ARIAS
SCHOOL OF POLICY, GOVERNMENT, AND INTERNATIONAL AFFAIRS, GEORGE MASON UNIVERSITY

OCTOBER 2014

In May 2008, a gang of corrupt police took a group of reporters in Rio de Janeiro hostage, subjecting them to several hours of torture that included a "game" of Russian roulette and simulated murders. They coerced the reporters, who for several months had been investigating the gang for running an extortion racket in the Batan section of the city, into providing them with the passwords to their e-mail accounts, where they found copies of the reporters' field notes.[1] The police also had contacts who, by telephone, provided them with detailed personal profiles of the reporters that they used in their interrogation efforts. Eventually, the reporters were released, but, facing the real possibility of future violence from state agents, they went into hiding in other cities.[2]

This story is just one of many examples from the past decade of data security breaches involving reporters operating in different parts of the world. Given the threats to which they and other researchers are subject, scholars who work in highly violent, unstable, or repressive environments or who research politically or socially sensitive issues should give serious consideration to such threats. Indeed, with the rapid expansion of electronic networking, attacks by both state and non-state agents designed to obtain data are likely to increase in the coming years. Though often overlooked

in discussions of field research,[3] guarding data against loss or theft in the field, while traveling, through remote access unbeknownst to the researcher, and after returning home is crucial for the safety of researchers and of the research subjects who have placed their confidence in them.

While in no way exhaustive, this discussion outlines some of the key issues academics and practitioners should consider when conducting research under insecure and even dangerous conditions. While I will discuss certain hardware and software issues relevant at the time of writing, readers should keep in mind that technology in this area advances quickly, and they should maintain a dialogue with security experts at their own institutions and in their broader professional networks to understand the threats they will face when they go into the field, as well as be aware of appropriate resources for securing data. The goal here, then, is not to provide scholars with a specific set of procedures they should follow but, rather, a framework for thinking about the problems they may face so they can develop solutions appropriate to their own concerns and the locales where they will work.

I rely here primarily on consultations I held with experts in data security connected to international foundations and advocacy organizations as well as with independent experts. While these individuals were generous with their time, most expressed some concern about confidentiality, and so their names do not appear in this paper. I also examined documents related to data security. The resulting discussion touches on six topic areas: (1) data sensitivity, (2) threat assessment and data security protocols, (3) preparation for the field, (4) field operations, (5) returning home, and (6) additional considerations and resources.

DATA SENSITIVITY

Understanding the nature of data sensitivity is an essential first step in establishing a high level of data security. Researchers need to make an honest appraisal of the overall sensitivity of the data they are collecting. Are they, for instance, gathering data on ongoing illegal state or non-state activities that could put individuals in legal or physical jeopardy? Conversely, would their data collecting have no negative effect on research subjects, even if fully disclosed in the press? An array of possible points occurs between these two, some of which are summarized in table 1.

TABLE 1. Data Sensitivity for Types of Subject Populations

	Illegal Groups	State Actors	Individuals and Communities
Low risk	Information unrelated to illegal groups	Information state actors are largely uninterested in or that may already be published	Information individuals have no reluctance to share and would be happy to see in the press
Moderately low risk	Information regarding illegal groups that the groups may want to see published	New information regarding state actors that has not previously been published and does not appear to be problematic on its face	Information that may prove mildly embarrassing but would have little impact on family or work life
Moderate risk	Information regarding legal activities connected with illegal groups, such as legitimate businesses owned by accused criminals or illegal activities committed in the more distant past	Information critical of state actors or policy	Information that could create family, community, or work tensions
Moderately high risk	Information regarding illegal activities committed by illegal groups in the recent past	Information highly critical of state actors or policy	Information that could create serious family tensions or loss of work
High risk	Information on ongoing illegal activities	Information regarding abuses of power, other state crimes, or criticisms of a highly repressive regime	Information that could disrupt an individual's life, possibly leading to family breakup, social ostracism, or open violence

Knowing the overall sensitivity of data can allow researchers to develop a broad data security plan. The first phase in any such plan is to segregate the data adequately and develop a security protocol that seeks to protect individual pieces of data. Effective segregation involves storing data in files

that separate, as much as possible, sensitive information from identifying information and reduce the total storage of the latter.

A basic protocol for separating sensitive data from identifying data is to use blind identifiers, such as pseudonyms, in the databases or notes that contain the sensitive information. Researchers can then maintain a second file to store identifying data they may need for reconnecting with research participants or for other research purposes. Finally, researchers can maintain a third file containing a key that allows them to link the sensitive data directly to the identifying information.

As the chance of identification is lowered overall, levels of risk diminish. Nevertheless, researchers should acknowledge the possibility that a subject could be identified through a host of means. Different pieces of data with different levels of sensitivity can be dealt with differently. The data key—the most sensitive—should be stored in the fewest and most secure settings, with unidentified data having a lower level of security. The researchers' understanding of the risk levels of their data will determine how they will store them.

THREAT ASSESSMENT AND DATA SECURITY PROTOCOLS

Before they go into the field, researchers should develop a threat assessment and a viable security protocol that will enable them to carry out their research with a high degree of security.[4]

Scholars should keep in mind that establishing absolute data security is impossible. This was the case forty years ago, when security agents could break into the home of a researcher to steal paper files, and it is certainly the case today. A flash drive containing thousands of pages of information can be quietly carried away without the researcher's becoming immediately aware of the loss. External hackers can gain access to a computer to upload large portions of a researcher's hard drive without the researcher's ever becoming aware the files have been taken or that the computer has been accessed. Governments with sophisticated information technology systems can comprehensively monitor significant portions of national electronic communications, using programs to sift through data for potential threats. State agents can also target individuals' data through targeted data monitoring or physical seizure of their electronic devices.[5]

Well before traveling to the field, and once they have determined the potential risks of the different data they will be dealing with, researchers should develop a realistic assessment of the data security threats they might face during and after research. They should consider who their opponents might be and what capacities they may have to breach their data. Under some circumstances, for example, physical theft of hardware may be the leading danger, while in others pervasive government monitoring and data censorship may be a greater cause for worry.

In addition to the privileged access state actors may have to electronic communications, many private actors, including criminal organizations, can gain remote access to data by hacking into secured computer systems using commercially available products.[6] Indeed, software today not only can allow both official and nonofficial hackers full access to computers; it can enable them to operate microphones and cameras installed in the computers without the users' knowledge.[7] Moreover, at present the ability of sophisticated actors to breach data appears to be growing at a far faster rate than the ability of individuals to secure them. The types of security measures undertaken should focus principally on the main threat a particular researcher faces.

Besides gaining an understanding of the specific actors who might pose threats to data, scholars should critically assess the types of devices they will use while in the field and where and how they will use them. In general, the fewer devices a researcher uses, the fewer the opportunities for an electronic data breach.

Researchers today are likely to carry personal computers. Those who do should consider the technical specifications of these devices and, in particular, whether they can manually cut Wi-Fi services to prevent unwanted remote access. Researchers should consider using two computers—one that connects to the Internet, which the researcher carries publicly but keeps very little data on, and a second, which the researcher stores sensitive data on and leaves in a secure location. Other electronic devices scholars may use that may expose them to risks include peripheral devices, such as scanners, printers, and facsimile (fax) machines (which have their own memory and storage capacity), and digital cameras and voice recorders.

Finally, of course, scholars should consider their communications options. Do they plan to use standard or "smart" cellular telephones? Smart phones,

which constantly stream data to the Internet and also store a large amount of e-mail and social media data, pose particular security challenges. Most portable telephones have global positioning system (GPS) capability that can be used to track users' movements.[8] Do they plan to use public Internet cafes or only secure, privately controlled Internet connections for e-mail and other web traffic? Closely assessing all electronic devices brought into the field and how and where researchers plan to use them can help them develop a plan to manage their risk profiles.

To build rudimentary risk profiles, scholars should critically assess what threats they might face and who poses them. The first step is to consider who may seek to gain access to the data and ways they might try to obtain them. Aside from the possibility of inadvertent loss, the researcher may be subject to an array of targeted attacks, such as spear phishing, man-in-the-middle attacks, physical assault, and broad-spectrum data collection. Table 2 offers examples of some different types of attacks, the risks they pose, and potential responses. The list is, of course, not complete, and the types of attacks and their relevance to a particular user can change over time.

TABLE 2. Types of Threats

	Definition	Examples	Responses
Broad-spectrum data collection	Large amounts of data are acquired by powerful agencies that automatically sort data to identify targets for further investigation	US National Security Agency monitoring; Internet monitoring by the People's Republic of China	Avoid connecting computers to the Internet; avoid use of identifiers in transmissions
Targeted electronic attack	Opponents engage in any one of a number of electronic activities to gain access to data on a computer and/or control of the computer	Directed attacks to install malware on a computer that may enable control of the computer even when the computer appears to be turned off; opponents may work with legitimate service providers to install such information on the user's computer	Firewalls; care when opening e-mail; strong data compartmentalization; virtual private network (VPN); browser anonymity

	Definition	Examples	Responses
Burglary	Physical entry to space where electronic devices are secured	Opponents enter secure space either to steal data or to install software to allow monitoring of the computer	Secure apartment; maintain high levels of security on devices; maintain compartmentalized data
Physical assault or theft	Physical or surreptitious theft of device	Bag containing device stolen; government agents or other armed actors seize device	Limit time devices are in public space; compartmentalize data; do not travel with data on device; transmit data to cloud before travel
Inadvertent loss	Researcher loses device	Data key falls out of pocket	Effectively compartmentalize and secure data; travel with minimal data on devices

The second step is to list each possible threat and source of data loss, along with the particular threats to which the data on each device or in each application might be exposed, and the third is to develop mitigation strategies to address each of these threats. These could be broken down by category or device, as shown in table 3, which describes some of the types of devices researchers may use, their potential risks, and possible mitigation strategies.

TABLE 3. Device Risk Levels

Device	Device Risk Level	Use	Types of Risks	Responses
Desktop computer	Moderate to low	Storage of sensitive data	Targeted attacks; man-in-the-middle attacks; burglary	Effective software; regular malware and antivirus scans; encryption; maintain key data on separate device

Device	Device Risk Level	Use	Types of Risks	Responses
Laptop computer	Moderate to high	Typing field notes that do not contain information that identifies subjects	Theft; accidental loss; targeted attacks; man-in-the-middle attacks	Effective software; regular malware and antivirus scans; encryption; lock system; care when traveling with device
Flash drive	Moderate	Transporting secured data	Attack when inserted in computer; accidental loss; theft	Maintain data only temporarily on device; encryption
Smart phone	High	Communications and e-mail	Theft of device to obtain all data; broad-spectrum attacks; focused attacks to obtain data or communications; accidental loss	Do not use; use only with minimal data; encryption; use with password; turn off during meetings
Standard phone	Low	Communications	Theft of device to obtain phone book; use of geolocation systems to locate researcher; access phone book data	Regularly clear memory; do not store names with phone numbers; use different telephones for different activities
Peripheral devices (printer, fax, scanner)	Low	Various	Theft of data unknowingly stored in memory; burglary; malware	Clear memory frequently

Table 4 offers a matrix researchers can use to develop a data security protocol. Researchers should include in their action plans some or all of the measures described below.

TABLE 4. Threat Assessment Matrix

Type of Threat	Device	Level of Risk	Type of Data Stored	Mitigation
Broad-spectrum data collection	Desktop computer			
	Laptop computer			
	Flash drive			
	Smart phone			
	Standard phone			
	Peripheral devices (printer, fax, scanner)			
Targeted attack	Desktop computer			
	Laptop computer			
	Flash drive			
	Smart phone			
	Standard phone			
	Peripheral devices (printer, fax, scanner)			
Burglary	Desktop computer			
	Laptop computer			
	Flash drive			
	Smart phone			
	Standard phone			
	Peripheral devices (printer, fax, scanner)			

Type of Threat	Device	Level of Risk	Type of Data Stored	Mitigation
Physical assault	Desktop computer			
	Laptop computer			
	Flash drive			
	Smart phone			
	Standard phone			
	Peripheral devices (printer, fax, scanner)			
Inadvertent loss	Desktop computer			
	Laptop computer			
	Flash drive			
	Smart phone			
	Standard phone			
	Peripheral devices (printer, fax, scanner)			

Encrypt Your Hardware

Perhaps the most effective way to provide a minimal level of data security is to encrypt computer hard drives and external storage devices. Current versions of MS Windows and MAC OS have the capability to encrypt a computer's hard drive, but this feature must be separately activated. General computer password protection without encryption offers no protection to the data of a user who loses control of his or her computer.

It is important to keep in mind that full disk encryption requires a hard disk to have at least twice as much space as is taken up by the data stored on it. Thus, if a user has 100 gigabytes of data on a disk, encrypting that disk will require 200 gigabytes of space. Large-scale data encryption will lead to additional wear and tear on a hard drive and decrease its useful life. Besides the built-in software that comes with major operating systems for hard disk encryption, researchers may use products such as Truecrypt to

provide additional encryption of sensitive files and to encrypt external hard drives and flash drives.[9] Researchers preparing proposals should consider the additional costs that data security imposes. These include maintaining multiple computers for different purposes and the wear and tear that encryption may cause hard drives.

Use Adequate Antivirus and Malware Programs

Researchers should maintain adequate security on their computers to prevent infection by dangerous software, such as viruses, malware, and spyware, that may try to install themselves on the computer each time the user goes on the Internet. Users should regularly conduct scans for such hostile software.

Avoid Using Excessive Software to Secure Devices

While security software is advisable at key points, too much of it can incite users eventually to disable protection that has made use of their devices cumbersome, leading to new and unforeseen vulnerabilities. Excessive use of security software can also at times attract unwanted attention from state agents, who may wonder about the need for such high levels of data security.

Scale Down

A basic element of good security is simply to create a minimum of data that necessitate high levels of protection. Developing a suitable system of pseudonyms and using it consistently can dramatically limit the amount of sensitive data subject to threats.

Use Robust Passwords

High-quality passwords are an essential element in protecting data on cell phones, computers, or in email accounts. At present, a high-quality password should have at least twelve characters, including upper- and lowercase letters, numbers, and other typographical characters. These passwords should be changed with some frequency, at least once every ninety days.

Prevent Data Breaches

A researcher should remember that once a device has been removed from his or her control, all data on it should be considered compromised. As one contact interviewed for this paper put it, the first thing any interrogator tries to do is gain access to an individual's computer and Internet accounts, as these often contain more information than the individual can provide orally.

Several other interviewees mentioned that customs officials may briefly seize an electronic device on entry to or exit from a country with the express purpose of copying all the data on it. Laws in some countries, including the United States, require users to present government officials with computer passwords when requested.[10] Similarly, in countries or conflict environments where the rule of law is frequently disregarded by citizens or state officials, researchers may find themselves faced with an array of complex security threats. No matter how briefly devices are out of their control, researchers should treat all data on them as now being in the hands of the individuals or agencies that held them.

Consult with Data Security Experts

To develop an effective and appropriate protocol, researchers should work closely with colleagues at their institutions and with experts who have experience at their field sites. Within a university, other scholars, academic advisors, and the information technology (IT) department can provide valuable advice on how best to secure data effectively, as well as information about the resources the university may make available to help secure data. Similarly, individuals living and working at the field site, possibly including reporters familiar with the area, can be asked what measures they take to secure data and about the specific types of threats that exist there.

Develop Emergency Protocols

Data security protocols should include emergency provisions if data become compromised or if the researcher is kidnapped or detained, some elements of which should be part of a wider emergency protocol for the entire research project. They might include provisions for remotely erasing cell phones and, if possible, computers, and providing a trusted partner with

access to any data stored in the cloud[11] who can secure the data, as well as any critical e-mail or communications accounts.

Be Aware of Cloud-Based Risks

While most of this discussion focuses on securing data locally, considerable risks are also involved in data transmission. These range from government eavesdropping on Internet telephone calls to intercepting data in transmission or hacking into a cloud-based storage account. Researchers should be aware of the privacy policies of their cloud-based storage services. While some companies maintain strong security and privacy protections, others have more flexible rules. Researchers interested in maintaining remote storage should consider simply transmitting files to computers controlled by their home institutions. In many cases, encrypting data that are transmitted, maintaining encrypted data in the cloud, and using services that provide a higher level of encryption for communications and data storage may be necessary. Researchers should become familiar with different encryption methods and, in particular, with public key encryption (see below).

Never Lower Your Guard

Always remember that breaches of data security most often result from personal error rather than targeted attacks. The loss of an unsecured flash drive is a much more common source of a data leak than the theft of a laptop or the remote accessing of a hard drive or data stream by government officials.

PREPARATION FOR THE FIELD

After building a security protocol, a scholar should take actions necessary to implement it well in advance of travel into the field. Given problems that can develop with new hardware and software, as well as the learning curve necessary to work effectively with these products and follow the protocol, at least several weeks should be allowed to take the steps described below.

Acquire Hardware

Well before traveling, researchers should procure whatever hardware they feel is necessary and that is best obtained before traveling to the field.

Security issues aside, early acquisition, testing, and use of hardware is essential to ensure new devices are not defective and that the researcher knows how to operate them correctly.

While not always possible, acquiring a new computer that is completely clean of previously stored data is advantageous. Researchers who cannot obtain new ones may consider reformatting the hard drives of their current computers and reinstalling the operating systems, software, and files they need for their field research. Such efforts ensure there are no stray files saved on the computer of which the researcher is unaware, and they also increase the chances the computer is free of malicious software that could compromise security. Especially in situations where researchers plan to take their computers to interviews, frequently traveling with them in public, acquiring a second computer may be a good idea. Maintaining two computers allows the researcher to use one for taking notes and the other for storing and working on data in a secure location. A researcher may also use a second computer for online activity to avoid connecting a machine with sensitive files on it to the Internet, thereby diminishing the chances of remote attacks on data.

Implement Software

Installing, testing, and beginning to use the software, especially encryption software, researchers plan to operate in the field before they travel there is essential. Encryption should take place as early as possible, since full encryption can take a while and requires a large amount of disk space. If the hard drive contains too much data, information will have to be deleted to undertake this type of encryption.

Researchers should also familiarize themselves with other file encryption and Internet security software they plan to implement. They should consider putting up firewalls that may offer some protection from attacks coming over the Internet.

Consider the Use of Broader Internet Security Tools

Those seeking basic, if slow, anonymous web browsing software may consider using the Tor Browser. It works within the broader Tor system of distributed network nodes that help mask users' identities by encrypting the routing information in Internet communications through a regularly

changing network of computers that are part of the Tor network.[12] The process of masking routing requests by sending those requests through multiple computers slows information movement.[13] This system can provide users with important protections against mass and targeted data mining.

Those needing a more sophisticated and smoother anonymous browsing experience may investigate setting up a virtual private network (VPN). With this system, the user maintains a separate router for remotely connecting to the Internet. When the user accesses the Internet they use the local, public, Internet connection to log in to their VPN on a remote server. Web browsing and data transfers are then sent to the VPN as encrypted traffic. The VPN then transposes the information and sends it back to the Internet as unencrypted data. Reponses return to the VPN router where they are again encrypted and sent back to the user. The result is that the owner of a public Wi-Fi or a third party who has gained access to the network only sees encrypted traffic going into and out of the user's computer.[14]

VPNs are extremely useful and can provide an important layer of protection to augment users' security while they are traveling. Users need a high level of technical expertise to set up such a network, install the software to access it, and learn how to operate within it, however; those who do not have such expertise should consult with their institutions' IT departments.

Establish Passwords and Accounts

Researchers should set up any new service accounts and establish new passwords several weeks before traveling to the field. New e-mail and Internet telephone[15] accounts for use in the field or certain key communications are advisable; users should avoid unnecessary use of these accounts and set up separate passwords for them. Implementing secure passwords in advance allows adequate time to become familiar with them. If necessary, researchers should use software or develop alternative methods for securely recording passwords in case of loss.

Clean Devices, Create and Transfer Files, and Encrypt as Necessary

In the days just before traveling to the field, the researcher should conduct a final data cleaning of all devices, including computers, flash drives, portable

hard drives, printers, and cellular phones. Remember that a "smart" telephone, even if not used in the field, likely has a large amount of information stored on it associated with contacts, e-mails, or social media. Depending on local conditions, a wipe of such a device may be advisable. Alternatively, researchers may choose to leave the device at home.

Before cleaning, the researcher should transfer any needed data to devices that are absolutely necessary for work in the field and encrypt them. Such information might, for example, include any lists of local contacts.

Some security experts advise avoiding crossing borders with any data saved on a device. Key information can be sent as encrypted files, via either a secure e-mail or cloud storage service. Before sending files in such a way, a researcher should ensure the service is using adequate encryption and be aware of the level of security provided. Under certain circumstances, researchers may consider sending encrypted files on a physical device via a courier service, such as DHL.

Get Training

Establishing basic security is not so complex, but how to do it is hardly self-evident. Researchers working with secure data should seek training to help them understand and technically manage information security issues. Solutions beyond the most basic require some comfort in working with technology, and researchers must be confident in their ability to use new systems and tools to maintain the security of their data as threats evolve.

FIELD OPERATIONS

Once on the ground, researchers should rigorously follow their data security protocols. If, however, problems develop with a piece of software or hardware, or the protocols prove unworkable or inadequate to thwart the types of threats they find themselves facing, they should consider judicious revisions that will enable them to maintain the intended level of security. They should keep a close eye on the security environment and, if necessary, initiate emergency data security plans and/or exit the field if extraordinary risks to themselves or their research subjects arise. This section will address hardware security, Internet security, mobile wireless security, and security implementation strategies.

Hardware Security

The most common risk to data is losing control of the devices on which they are contained. Even in the absence of any meaningful external threats, it is easy to lose a flash drive, and expensive laptops are tempting targets for thieves, especially when researchers are traveling or keeping the devices in temporary apartments and offices. The most basic ways to maintain data security under these circumstances include ensuring office and apartment doors are kept locked and that devices containing sensitive data are kept inside locked cabinets, desks, or, if possible, safes.

While good data management includes maintaining appropriate backup copies of files, researchers should seek to minimize the number of places in which they store data. Scholars should consider whether they really need to travel with their computers on any given occasion. Computers regularly brought into public spaces are exposed to greater risks than those that remain secured at all times. A researcher who will regularly need a computer for note taking should consider not keeping sensitive data on that computer.

Similarly, while backing up data on a regular basis is good practice, it is important to maintain limited copies of sensitive data. The fewer copies that are available and the more secure they are kept, the less chance data loss will occur. Scholars working with sensitive data should ensure all are encrypted and made anonymous. Although (as mentioned earlier) some researchers may disagree, in general, the most effective and reliable way to accomplish this, especially for those lacking in technical expertise, is to fully encrypt any device that contains such data. Researchers with knowledge of encryption techniques can adopt more complex encryption strategies, including hiding particularly sensitive files within other files to make them harder to find and access.

Finally, computers should be completely shut down when they are not in use. Doing so ensures the files are fully encrypted and password protected.

Internet Security

Internet security and hardware security are closely connected. Computers connected to the Internet through Wi-Fi, cellular communications, Bluetooth, or physical connections are exposed to external hacking. These attacks can come in the form of e-mails with links that install malware on

the target computer, giving outsiders access to the computer's data and transmissions.

Attacks can also come from local wireless service providers' systems. Hotel Internet systems and Internet cafes do not offer users secure connections. Users should take care when transmitting data over them and when connecting their hardware. The most secure way of avoiding these types of attacks is never to connect a computer containing sensitive data to the Internet; researchers may simply maintain a separate computer for this purpose. Users may consider storing sensitive data on a peripheral device, such as an external hard drive or a flash drive, and only connect it when the computer is disconnected from the Internet.

As mentioned above, users with sufficient technical expertise and infrastructural support may use a VPN to avoid having their Internet activities tracked by outsiders. Field researchers who use public computers may employ the TAILS operating system, which can be installed on a USB drive or DVD and then serially used on different computers. This system allows users to exploit Tor networked anonymity on third-party computers and anonymously engage in other computer activity, such as word processing, through an operating system that runs independently of a computer's hard drive. Once the flash drive is removed and the computer is restarted, all traces of the work conducted under TAILS should disappear.[16]

A second challenge related to the Internet is communications. Contacts made via the Internet are generally less secure than those made in person or over the telephone. E-mail services maintain long records of data transmissions and are exposed to greater legal risks than telephone companies. Some contacts in highly sensitive places may refuse to communicate via the Internet, and researchers should respect their choices.

Users of Internet communications as well as cloud storage services should be aware of the legal protections and security protocols they maintain. Google, for example, makes public its privacy policies and also the number of times it has been asked to produce user data for specific countries. Researchers may use secure e-mail and browser services as well as VPNs to augment the security of their communications and those of their subjects. They may even consider recommending that subjects and other contacts adopt secure communications protocols.

Internet cafes are not secure places to transact sensitive e-mails or other such communications activities. Researchers may want to consider having segregated e-mail accounts for sensitive and nonsensitive communications if they believe they may be dependent on Internet cafes or public computers for social communication.

For e-mail and other accounts that are used for sensitive data transmissions, scholars should consider using two-step verification for sign-in. A user who signs into an account with this process is sent a code via short message service (SMS) or some other means. The user then must provide this additional piece of information to obtain access to his or her account. The two-step verification minimizes the chances that a compromised password will lead to unauthorized access to the account.

Cellular Telephone Security

Cellular telephones pose important data security challenges for researchers. Most relevant to this discussion are smart phones, which are largely insecure devices that contain and regularly transmit large amounts of data via e-mail and social media services. They can also act as flash drives.

Scholars should be aware of the information contained on their telephones, the danger of losing them, and the broader risks of continuous data transmission in situations where state agents or other technologically sophisticated actors may seek to access the phone's data or geolocation information. When working with sensitive data, scholars should consider simply avoiding the use of smart phones. To the extent they do use them, they should consider encrypting the files on the phone and installing software allowing it to be reformatted remotely to remove all data should they lose control of the device. When holding sensitive meetings, researchers should turn these devices off to avoid being externally monitored or tracked.

More limited cellular telephones likely provide a greater degree of security. Users of these telephones should be aware, however, that both regular and smart cellular telephones when turned on can be used to locate them. In highly sensitive environments and at particular times, users should consider turning off their telephones to address geolocation concerns.

Implementing Emergency Procedures

A basic data security protocol should be included within broader emergency exit and safety protocols. A data security protocol should empower a key contact to wipe any devices remotely and secure information associated with the project that may be accessible over the Internet. This may involve, as appropriate, changing passwords and downloading and deleting data that may be exposed should the researcher be unable to take care of this in an emergency. Researchers should investigate remote device deletion technologies they can use in the event they lose their devices. Those who lose control of sensitive identifiable data should contact individuals who may be affected by the loss.

RETURNING HOME

Exiting a highly violent research locale can provide researchers with a measure of security. Universities themselves are often located in safer regions with greater state capacity and, even when close to a research site, provide higher levels of security. More importantly, perhaps, the end of ongoing intensive field research puts space between the researchers and subjects that can begin to reduce external interest in the research prior to its publication. The data analysis, writing, and publication portion of any research project, however, entails its own risks. Scholars who conducted research in their home cities or countries and those who did their field work overseas both continue to confront some types of data security threats even after they have left the field. These are summarized below.

Issues for Researchers Working in Their Home Countries

Local researchers, especially those who live and work in conflict areas, face considerable risks even after the conflict has ended. During the 1980s and '90s, for instance, violence researchers at the University of Antioquia in Medellin, Colombia, suffered numerous threats, and some were murdered.[17]

Post-field data security should be a major concern for locally based scholars. State agents and others interested in their data can often gain access to their offices and universities and, depending on local laws, may be able to take legal or administrative actions to obtain the data.

Researchers should be aware of the types of legal risks they may face and should also, to the extent possible, work with their own institutions' administrations to maintain adequate safeguards on data and ensure support in the event legal action, such as a subpoena for data, is taken against the researcher.

Scholars working near their field sites should consider maintaining many of their basic field work security protocols even after they have completed research. Generally speaking, this involves keeping to a minimum the number of copies of the data, ensuring that identities remain segregated from data in other coded files, maintaining encrypted hard drives, and storing all data in secure locations. Extra copies on flash drives or external hard drives should be kept in locked cabinets. A researcher who is concerned about a sophisticated remote threat to his or her computer should try to analyze data on a separate computer not connected to the Internet. Scholars should also work with their local IT departments to monitor their computers regularly for the presence of invasive software that could compromise security.

Issues for Researchers Working outside Their Home Countries

The immediate concern for researchers working outside their own countries is returning home with sensitive data. Border crossings are important opportunities for security officials to gain access to data and, for that matter, anything else a researcher is carrying. Border officials can easily seize a researcher's computer or cellular telephone and download and/or erase the contents of the device before allowing the researcher to move on. As mentioned earlier, laws in some jurisdictions, including the United States, may require individuals to disclose their passwords to border officials.[18]

Under some circumstances, it may be inadvisable to cross an international border with any sensitive data on a computer. In this case, two principal avenues can be used for moving the data. Assuming good Internet connections are available, they can be uploaded to a cloud drive. Data sent in this way should be fully encrypted to ensure its security. The encryption of the data can be heightened through the use of public key encryption, in which the password to encrypt the data is different from the password needed to decrypt the data.

If a good Internet connection is unavailable, a scholar may consider saving encrypted data on a flash drive and mailing it to him- or herself via an international courier service, such as DHL. As discussed above, researchers should employ high-quality encryption for this process and consult IT services on their campuses regarding encryption options. As also mentioned above, at the time of this writing Truecrypt offered a free, publicly available encryption product.[19]

Once back home, researchers should consider maintaining as much of their field security as practicable. This may be particularly important in situations in which they face technologically sophisticated remote threats, and sensitive data are best examined only on computers not connected to the Internet, if possible. Beyond this, scholars should consider working with their local IT departments to ascertain their levels of security and determine how to raise or maintain them.

ADDITIONAL CONSIDERATIONS AND RESOURCES

Beyond the broad set of security issues discussed in this paper, researchers should also consider the legal and institutional issues affecting data security as well as the broader limits of security. This section briefly examines these issues and offers an outline of other resources that may be helpful to researchers as they move forward in building data security plans.

Legal Issues and Institutional Ethics Boards

Scholars should be aware of the key legal and ethical issues that concern them in both their home countries and the countries where they are conducting research and the types of legal jeopardy to which their research can expose them, their subjects, or their institutions. In the United States, scholars can obtain a Certificate of Confidentiality from the US Department of Health and Human Services that offers them some protections from being compelled to disclose data in federal and state legal proceedings.[20]

Scholars should also, to the extent possible, be generally aware of the underlying protections offered and privacy postures assumed by providers of different web services and applications. As mentioned above, Google maintains transparency information indicating the number of cases in which they have divulged user data. When transmitting information on the Internet,

researchers should be sure to use secure Internet sites with the prefix *https*, as opposed to *http*.

Limits of Security

As indicated earlier, it is impossible to maintain complete data security, and scholars need to be aware of the limits. Maintaining notes that are not traceable to individuals is a key strategy to keep data from reaching others. Scholars should develop security protocols appropriate to their situations but not implement excessive protocols or use unnecessary software that might actually limit their ability to maintain security. They should follow their security protocols as closely as possible.

Other Resources

Scholars interested in developing greater awareness in the area of data security should consult with different organizations that can provide them with technical assistance and training. Key to this process are local IT departments that may be able to aid scholars in their efforts to increase data security in a number of the ways that have been discussed here.

In addition, Reporters without Borders has conducted extensive research into how reporters can best secure their data. They maintain a substantial amount of information on their website.[21] Reporters without Borders also runs trainings for journalists and at journalism schools, providing reporters with basic information about data security. In the United States, the Open Technology Institute of the New America Foundation also provides useful advice.[22]

CONCLUSION

No foolproof way exists to secure data. Devices used by researchers have proliferated rapidly, and each has different vulnerabilities. While this discussion has gone into some detail regarding a broad array of security threats and ways of protecting data, it is critical to remember that the most typical threat to data is the loss or theft of a device. Researchers need to maintain basic encryption on their devices as well as keep effectively anonymous notes to reduce the exposure of informants should they lose control of their

work. Beyond this, users need to be aware of the broader array of threats and, as necessary, maintain security against them.

NOTES

1. I thank Javier Osorio and Camino Kavanagh for their insightful comments on an earlier draft of this paper.

2. Enrique Desmond Arias, "Dispatches from the Field: Milícias and Police Corruption in Rio de Janeiro," *Americas Quarterly* 3, no. 2 (2009): 90–93.

3. For a discussion of some perspectives on these issues, see Wendy S. Davis and Samantha Eldridge, "Privacy, Confidentiality, and Data Security in the Age of Electronic Records and the Internet: Implications for 'Human Subjects Review' in the Social Sciences," paper presented at the Western Political Science Association Conference, Portland, OR, March 22–24, 2012.

4. The Committee for the Protection of Human Subjects at the University of California at Berkeley has developed a good baseline threat assessment tool. It can be found at http://cphs.berkeley.edu/datasecurity.pdf.

5. On data theft in earlier times, see Janice Perlman, *Favela: Four Decades of Living on the Edge in Rio de Janeiro* (New York: Oxford University Press, 2009); Heather Brooke, "How the US Government Secretly Reads Your E-mail," *Guardian*, October 11, 2011, http://www.guardian.co.uk/commentisfree/cifamerica/2011/oct/11/us-government-secretly-reads-your-email.

6. On Mexican cartels and data security, see José Abreu, "Mexican Drug Cartels and Cyberspace: Opportunity and Threats," *Infosec Institute*, March 21, 2012, http://resources.infosecinstitute.com/mexican-cartels/, accessed June 18, 2014.

7. Askan Soltani and Timothy B. Lee, "Research Shows How MacBook Webcams Can Spy on Their Users without Warning," *Washington Post*, December 18, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/, accessed January 3, 2014; for a more detailed discussion of state and non-state targeted applications of this type of software as well as possible responses to its use, see Albert Fruz, "Remote Access Tool," *Infosec Institute*, April 24, 2014, http://resources.infosecinstitute.com/remote-access-tool/, accessed June 18, 2014.

8. On issues related to smart phones, see Marcel Rosenbach, Laura Poitras, and Holger Stark, "iSpy: How the NSA Accesses Smartphone Data," *Speigel Online International*, September 9, 2013, http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html, accessed January 3, 2014.

9. Under some circumstances, experts advise using separate encryption software for specific files rather than full disk encryption. Given the information that becomes available

in file registries as a result, however, such an encryption strategy is only advisable for sophisticated users, and only in situations where a user believes full disk encryption might attract unwanted official attention.

10. Lisa Vaas, "US Customs Can and Will Seize Laptops and Cellphones, Demand Passwords," *Naked Security*, January 9, 2012, http://nakedsecurity.sophos.com/2012/01/09/us-customs-can-and-will-seize-laptops-and-cellphones-demand-passwords/, accessed October 7, 2013.

11. Here "the cloud" refers to the remote storage of data files accessible through the Internet. Services such as Dropbox, Google Drive, iCloud, SpiderOak, and Tresorit provide remote Internet accessible data storage. All services come with different levels of security and features, and some are markedly insecure. Their mention here does not constitute an endorsement by either the author or the SSRC.

12. See Tor, "Tor: Overview," https://www.torproject.org/about/overview.html.en.

13. See Tor, "Tor: FAQ," https://www.torproject.org/docs/faq.html.en.

14. Eric Geier, "How (and Why) to Set Up a VPN Today," *PC World*, March 19, 2013, http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html, accessed June 11, 2014.

15. While this discussion is intended for scholars of Latin America, others reading it should be aware that the version of Skype available for use in China at the time of writing—often referred to as Tom Skype—was designed to provide the government with access to its users' communications and is not recommended for secure contacts. Readers should keep aware of changes in software and web products that may compromise security.

16. For information on this product, see https://tails.boum.org/about/index.en.html.

17. Mary Roldan, *Blood and Fire: La Violencia in Colombia, 1946–1953* (Durham, NC: Duke University Press, 2002), 1–3.

18. Susan Stellin, "The Border Is a Backdoor for US Device Searches," *New York Times*, September 9, 2013, http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html?pagewanted=all, accessed January 3, 2014; also see Matt Villano, "Border Agents Limit Confiscation of Laptops," *San Francisco Chronicle*, September 13, 2009, http://www.sfgate.com/travel/article/Border-agents-limit-confiscation-of-laptops-3286821.php, accessed January 6, 2004.

19. See http://www.truecrypt.org/docs/ and https://tails.boum.org/about/index.en.html.

20. See http://www.hhs.gov/ohrp/policy/certconf.html.

21. http://en.rsf.org.

22. See http://oti.newamerica.net/.

ABOUT THE AUTHOR

Enrique Desmond Arias is an associate professor of public policy in the School of Policy, Government, and International Affairs at George Mason University. His research focuses on security and politics in Latin America and the Caribbean. He is the author of Drugs and Democracy in Rio de Janeiro: Trafficking, Social Networks, and Public Security *(University of North Carolina Press, 2006); coeditor of* Violent Democracies in Latin America *(Duke University Press, 2010); and principal author of the* Introductory Handbook on Policing Urban Space *(United Nations Office on Drugs and Crime, 2011). His writing has appeared in* Comparative Politics, Perspectives on Politics, *the* Journal of Latin American Studies, Policing and Society, Qualitative Sociology, Latin American Politics and Society, Studies in Comparative International Development, *and the* Revista de estudios socio-juridicos. *He is currently writing a book on the impact of gangs and other armed groups on politics in Rio de Janeiro, Brazil; Medellín, Colombia; and Kingston, Jamaica. The US Fulbright Commission, the American Council of Learned Societies, the Tinker Foundation, the National Consortium for the Study of Terrorism and Responses to Terrorism, and the Harry Frank Guggenheim Foundation have provided funding for his research. Arias is series editor of the DSD Working Papers on Research Security.*