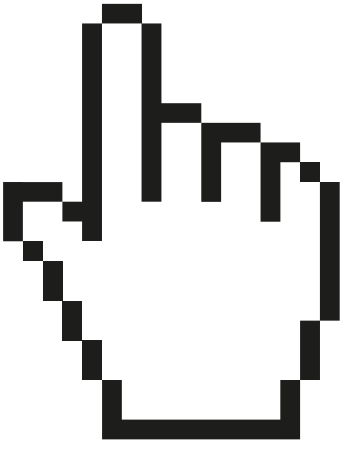
Access of public authorities to the data of Internet service users

Seven issues and several hypotheses



PANOPTYKON FOUNDATION

An attempt at summary

For several years now a discussion has been underway in Poland concerning the use of telecommunications data (billings, location data) for the purpose of combating crime. Thanks to this public debate, we have managed to diagnose several crucial issues at the intersection of human rights, security policy, and the interests of private companies. The Ministry of the Interior is presently trying to solve some of them by proposing amendments to the applicable law.

Of course, government authorities request not only data processed by telecommunications operators, as companies providing services by electronic mean must also respond to such demands[1].

Whenever the state requests data belonging to its citizens, data which they have entrusted to private companies for an entirely different purpose, it is obvious that problems arise – and at the very least, serious dilemmas. Expecting to encounter a great deal of such issues in the area of Internet services, we decided to take a closer look at the principles which govern the transfer of personal data belonging to citizens – who at the same time are users of such services – when various governmental authorities make such requests.

Who is filing requests, and for what information? What is the scale of such requests, and does it really matter? In what manner are requests addressed to companies? What legal grounds do public authorities most often make avail of? Is the obligation to disclose data upon the demand of government authorities burdensome from the perspective of companies? How much does it cost, and who pays for it?

With these questions in mind, half a year ago we launched a project aimed at learning more about what is going on at the interface of Internet service providers and public authorities. Thus, for the past months we have been analyzing legal provisions, talking to businesses and government bodies (mostly to the police), formulating ever more detailed questions, and collecting data.

We do not offer many ready-made answers – rather, we propose hypotheses which need to be verified. We hope that the information and data we have gathered will mark the beginning of renewed public debate and inspire further research activities.

Our partners in this endeavor were four companies that provide Internet services: Agora, Google, INTERIA.PL and Onet (in alphabetical order). In accordance with the law, none of these companies is obliged to record and submit reports on data requests made by public authorities. So, if it weren't for their good will, it would not have been possible to learn about the practice of applying the regulations which oblige companies to make data available to governmental authorities. Therefore, we value their helpfulness all the more.

---

[1] This category includes all Internet services: providers of electronic mail services, hosting, forum administration, shopping and auction portals, browsers, all types of communicators, and Internet portals (even non–commercial ones). Activities of this type are regulated in the Act on Providing Services by Electronic Means (APSEM).

This study is an attempt to collate and summarize the findings from that process, one which – due to its limited range and exploratory nature – often tables more questions than it gives unambiguous answers. Nonetheless, this had great cognitive value for us. We encourage everyone to become familiar with the conclusions which we publish here, our intention being to launch necessary debate and to inspire research activities on a wider scale.

Goals: what did we wish to achieve?

Our aim was not to collect and present raw facts on the scale of user data requests directed by public authorities to online service providers. The experience we gathered during the debate on access to telecommunications data taught us that such figures are not the most important. Comparisons we prepared of data from different sources, along with the recent report of the Polish Supreme Audit Office, have shown that despite the obligation imposed on telecommunications operators to make reports, their statistics are kept without a coherent methodology and are therefore unreliable. As a result, they can be misleading and draw our attention away from more serious problems.

It is not our aim to stigmatize companies which – while operating within the legal framework – process requests to disclose user data. The fact that they adhere to the law deserves recognition. If, at the same time, they also show concern for transparency, their customers may feel reassured. But on the other hand, citizens simply have a right to know more about the principles according to which companies must cooperate with governmental bodies.

Our aim is to launch serious and thorough-going public debate. In this context, it is essential to understand and present the problems connected with the access of the police, courts, prosecutor's office, and government authorities to data processed by online service providers. Therefore, the following questions were given primacy: Are the existing procedures sufficient? What is the practice of government authorities – which legal grounds do they most often draw upon? Do most requests appear to be justified in the opinion of companies? Is there a need to introduce new mechanisms of control over the activities of the police and other authorities? What costs are incurred by Internet service providers, and are they justified?

Our aim is to initiate public discussion on the principles for disclosing the data of Internet service users to government authorities in order to improve these principles. Diagnosis of the existing problems offers merely an introduction to joint deliberations on how to solve them by amending the law and making its provisions more precise.

We hope that this initiative – with the participation of four important companies present on the Polish market – will mark a beginning of a new trend; that with time all market-leading Internet service providers will agree that it is worth answering questions before they are asked, and worth openly talking about the principles for disclosing data upon the demand of public authorities. Holding an open debate on this subject should be beneficial for all the parties involved. By juxtaposing the perspectives of companies, citizens, and government authorities, we are able to diagnose problems which affect everyone. Moreover, these problems prove to be resolvable.

Context:
from the debate on telecommunications data to "the wiretapping scandal"

Our direct inspiration for taking a closer look at the practice of disclosing the data of Internet users was that of the conclusions drawn from the public debate concerning the use of telecommunications data by public authorities. After more than three years of discussion on that subject, we still have many unknowns. The largest ones regard the accuracy and reliability of the statistics generated by the Office of Electronic Communications, which have recently been brought into doubt by a devastating report of the Supreme Audit Office. Thus, we now realize it is even more difficult to specify for what purposes governments use telecommunications data and what type of data they request from operators.

Despite all these unknowns, we managed to identify several specific problems – primarily, that there is no supervision by an independent authority over who submits requests directed to operators, for what purpose, and for what type of information. In response to the problems identified, the Ministry of Internal Affairs declared the intention to introduce amendments to the applicable law – in particular, to create the Special Services Audit Committee. Moreover, the public debate featured certain themes important for companies, such as the issue of cost reimbursement and the need to streamline the procedures applied by the authorities which request data. Perhaps the next step is that lawmakers will address these problems.

Our experiences in the debate on the principles governing the disclosure of telecommunications data convinced us that the interest of the media and opinion-makers in a given subject can be very beneficial – even if this means dummying things down. Indeed, it seems that there is simply no other way to improve the existing legal framework. Hence the idea to publically take up the issue of the privacy of Internet service users in the context of the activities of judicial, prosecuting, and other public authorities.

That decision coincided with the disclosure that US authorities had gained large-scale access to data stored by the largest Internet companies. However, this study – placed in the framework of Polish law – is not a voice in the discussion evoked by the revelations of Edward Snowden.

US law provides that the data of customers of companies subject to American jurisdiction may be made available to government agencies practically without limitations, so long as that the customer is not a citizen of the United States. Despite there being no independent controlling mechanisms over the operation of Polish authorities, they must always justify their demand for data disclosure on the basis of relevant legal grounds. Neither the legal provisions, nor the experience of the four companies give reason to think that in Poland we are facing mass surveillance of Internet service users. We support this statement in a detailed description of the principles for disclosing data in the second part of this study.

* * *

Due to the unique features of the collated material, we have divided our study into two – largely independent – parts:

- **the first** constitutes an attempt to interpret the data which we received from the four companies in the framework of a pilot study, and from government bodies (mainly agencies) in response to requests for access to public information; moreover, the data collected from telecommunications operators by the Office of Electronic Communications have been quoted to provide context;

- **the second** features the core issues – it collates our findings drawn from analysis of the legal provisions and from conversations we carried on at the stage of preparing and analyzing surveys with the companies providing Internet services, as well as from interviews with the police.

We hope you enjoy our report!

I. The practice of companies and government authorities: analysis of the data collected

In this part of the study, we:

- present information about the scale and practice of disclosing the data of Internet service users at the request of government authorities; we obtained this information thanks to our cooperation with four leading companies which provide such services;

- compare the answers of the companies with the information which we obtained from government bodies via access to public information;

- juxtapose the scale of disclosing Internet users' data on the demand of public authorities with the scale of disclosing telecommunications data;

- table several hypotheses which we deem worth examining and verifying.

I. Pilot study: what did we want to achieve, and where did we succeed?

The basic difficulty when assessing the scale and practices of requesting the data of Internet service users is that Polish law obliges neither the companies providing such services nor government bodies to keep statistics and prepare reports thereon. If companies do prepare such reports, they do so at their own volition in order to meet society's expectations. Counting on such openness, we decided to ask several questions to leading companies which provide Internet services on the Polish market.

Nobody before us had talked to such companies regarding data requests made by various government authorities. No wonder, then, that even those firms which were willing to cooperate with us had no uniform and systematized knowledge on the subject. In certain cases it appeared that the data which we were looking for indeed existed, but only in paper form, and to convert them to electronic format would be very time–consuming for the company concerned. Having learned of limitations of this type, we decided to begin by talking with companies and launching a pilot study. We wanted to verify whether we were asking questions in the right way, to check what data companies had at their disposal, and whether they were ready to share that knowledge.

Why would companies talk openly about their practices of disclosing the data of Internet service users on the demand of government authorities, if the law does not oblige them to do so? We wanted to check whether, following the model of multinational giants such as Apple, Facebook, and Google, Polish companies would also be willing to disclose certain statistics. We knew that if we succeeded, this would be the first initiative not only in Poland, but also in Europe, aimed at exploring the practice of disclosing data by companies providing services by electronic means.

Our aim was not to create a ranking of transparency among the firms involved, therefore the answers they provided have undergone pseudonymization[2]. We wanted to check how the provisions on obtaining information on Internet users function in practice, even if that would raise more questions than answers. We were aware from the beginning that it would be difficult to collect exhaustive data. Our aims focused on creating a coherent method which could be applied in further research activities on a wider scale, as well as on launching an open discussion on the principles for disclosing Internet user data at the request of government authorities.

We are not sure if all the data we managed to gather as a result of our cooperation with the four firms are fully comparable. However, we applied our best efforts to clarify all ambiguities and doubts at the outset. Before we began to prepare a survey form designated for the companies, we spoke with their representatives, and this helped us learn which data categories are collected by particular companies and to what extent the internal principles for data collecting and reporting are similar.

Conversations with companies – qualitative analysis
The companies which we invited to participate in this project were involved in it from the very beginning, including at the stage of preparing the surveys. We conducted interviews that helped us understand the principles behind the functioning of many processes and which are reflect in the description of the practice of applying legal regulations in Poland. The majority of specific problems described in the second part of this study was diagnosed precisely on the basis of consultations with the companies we conducted at the stage of preparing the survey form. That confirmed our assumption that learning about the mechanisms and principles on which disclosure of Internet users' data at the request of public authorities takes place is more important than a raw, quantitative analysis of the phenomenon.

The possibility of making a diagnosis of the problems and working out common conclusions proved to be more important than the scale of the data obtained.

Method

We invited twelve companies – the owners of the most popular Polish-language Internet portals – to participate in the pilot study. The companies were selected on the basis of research conducted by Megapanel PBI/Gemius (February 2013). A decisive factor was the position of the given company on the Polish Internet services market, measured by the number of users; we disregarded their location and origin.

[2] In this case: separating answers to surveys from the particulars directly identifying firms and replacing the latter with ordinal numbers.

Therefore, besides Polish companies, the group also included foreign businesses. A majority of the companies declared their willingness to cooperate, however, in the course of the project some of them resigned from participation.

At the initial stage, we spoke with representatives of the companies invited to cooperate with us, which fact not only helped us collect information on the practices of government authorities using data and the challenges arising in connection therewith, but also constituted bases for the preparation of survey forms which were subsequently given to the companies.

Each of the companies received two versions of the survey: a basic and an extended one. In the basic version, we asked about the information which – as we had learned earlier – a majority of them held: how many data requests did government authorities submit to them in the past year in total, and as divided into the types of such authorities? How many requests met with response in the form of disclosing the requested data? The extended version contained questions on the number of accounts to which data disclosure requests referred and the number of accounts in relation to which such data had actually been disclosed. In the survey we also asked how many times access was requested to specific data categories and how many times such data had actually been disclosed. These categories are: subscriber data, data provided during registration, login history, geolocation data, content of public communication, information on contact networks, and files in cloud storage.

The extended version of the survey also included questions concerning the legal grounds to which the public authorities referred when requesting data access, as well as the company's attitude when verifying the legitimacy of such requests. We asked about the procedure applied in the case of rejecting a request on formal grounds and whether the companies collect fees from public entities requesting data access. We were also interested in how time–consuming the processing of data requests is, and which information channels in communicating with public authorities are acceptable for a given company.

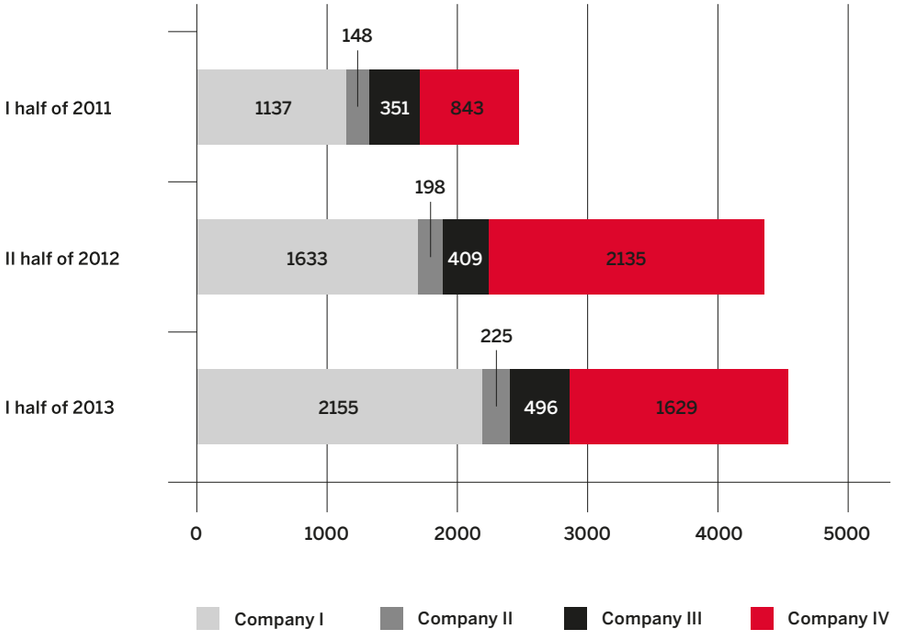
In order to supplement the information provided by the companies participating in the pilot study, we decided to ask the other party – the public prosecutor's office, the police, and other authorities – about the number of requests directed to online service providers. We received only several, individual answers, ones we present further in this study for illustrative purposes.

II. What do we know about the scale of data requests?

The discussion concerning how much government authorities want to know about their citizens and how this affects online service providers can easily be reduced to numbers. However, this is an unnecessary and dangerous simplification. It is not the scale which is important, but primarily whether public authorities make requests only when they have valid grounds, and whether companies respond only when they have to.

Information regarding the number of requests from public institutions was made available by all four companies taking part in the pilot study. The data collected for the analyzed 18 months are presented in graph 1.

Graph 1: Number of requests made by all authorized public bodies to Internet service providers (on the basis of data provided by four firms)



The answers provided show that the absolute number of data requests received by particular companies varies significantly. How can we explain these differences?

The first hypothesis which comes to mind is that the number of requests depends on the size of a company and the number of its customers. This no doubt holds to some extent. However, it is worth pointing out that each of the cooperating companies conducts its activity on a large scale and has a significant position on the Polish market. Conversations with representatives of the firms throw more light on the problem. They show that the key factor in this case is the business model and the type of services provided. The greater the number of possible disputes between users and potential breaches of the law, the greater the number of requests. For instance, a business model based on the sale of goods and services on the Internet in principle involves a greater risk of fraud and copyright–related disputes than one consisting in running an information portal combined with a discussion forum. In the latter case we might expect controversies between users in connection with infringement of personal rights, including defamation, and this less frequently engages public authorities.

Our consultations with the police – which, following the prosecutor's office, submits data requests most often – have shown that another significant factor is the location of the server and the jurisdiction governing a company. Foreign businesses present on the Polish market as a principle send the police and other government authorities back to their headquarters. Not all police officers manage to deal with such a procedure. If they have a choice, they prefer to ask a Polish company about the same issue. This is one reason why in the case of international corporations, such as Facebook or Google, the number of requests they receive may be lower than one would expect on the basis of the scale of their operations.

Analysis of the data provided by all the companies which participated in the pilot study leads to the conclusion that in the period we researched the number of requests from public authorities has been consistently rising. The question remains, however: what is the reason for that growth? Did the public authorities have more reasons to make requests (e.g., in connection with a rise in the number of proceedings involving customers of Internet service providers)? Many factors testify that this is the case.

Due to the fragmentary nature of the data analyzed, it is difficult to judge whether or not the increase in data requests is a broader and permanent tendency. However, our conversations with company representatives and the police suggest it is justified to think so. Much testifies to the fact that the rise in the number of requests for Internet users' data on the part of government bodies is a side effect of increased social activity on the Internet. Along with the transfer of various spheres of life to the web, crime is also moving there; likewise, the number of disputes between citizens arising from Internet activity is also growing.

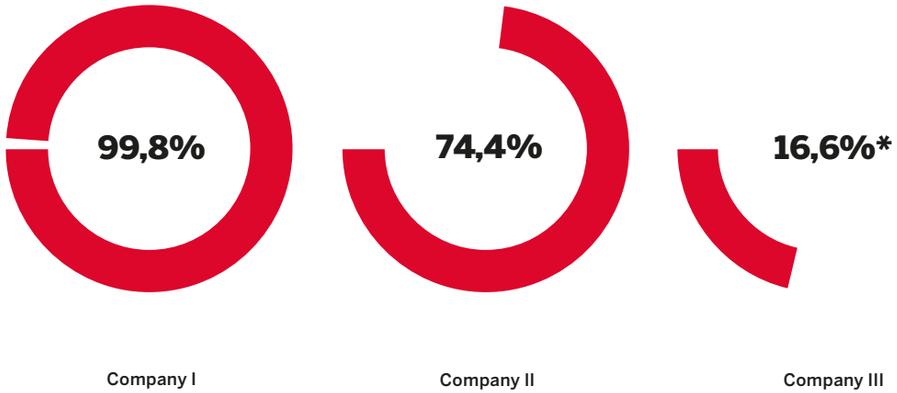
Such conjectures are confirmed by numerous research studies on the activity of Internet users over the past few years. The authors of the research of CBOS for 2012 state: "The number of internauts is rising dynamically – almost two–thirds of adults declare that they surf the web for non–professional purposes." The research of the World Internet Project conducted in 2010–12 also indicates that the percentage of Internet users in Poland is growing on a year by year basis. In 2012 two–thirds of the persons surveyed used the Internet, including over 90% at an age below 30. Research on the activity of children and young people, e.g., by the Inspector General for Personal Data Protection, along with research conducted by TNS in cooperation with the Orange Foundation and the Nobody's Children Foundation (Fundacja Dzieci Niczyje), show that the Internet is widely used by children, as well. We may venture to state that as the generations of active Internet users mature, the number of requests for their data for the purposes of various proceedings will also grow.

Why is the scale of data requests sometimes deceptive?
Our conversations with the police have proven that the scale of data requests in no way corresponds to the scale of the police's (or other public authorities') interest in particular citizens. This is a consequence of the practice of prosecution activities which in principle begin with a wide–scale search to narrow down at a further stage to the circle of suspected individuals. In order to specify the accurate IP number, it is usually necessary to verify or compare many others. However, that does not mean that the police is interested in everyone whose IP number was mentioned in the case files. That would be the shortest way to paralyze the work of law enforcement authorities.Additionally, the discussion on the scale of requests directed to companies providing Internet services is made difficult by the fact that there is no coherent method of reporting. How should we count such requests? Should a request for each IP number – even if it aims at specifying one culprit – be counted separately? What do we do when one request (e.g., for an IP number) subsequently generates more detailed ones (e.g., for the data provided by the user in the service agreement), but still refers to the same case? Doubts arise exponentially.

III. How do companies react to data requests?

A comparison of the number of requests made by public institutions with the number of answers given leads to interesting conclusions. It appears that in the case of three companies which were able to provide appropriate data **the percentage of disclosures is quite varied: from about a dozen to several dozen percent over 18 months**. The question as to where such large differences in the percentage of disclosed data may arise from remains open.

Graph 2: Percentage of user data disclosures by Internet service providers in response to requests of government authorities in the period 1.01.2012–30.06.2013 (on the basis of data provided by three companies)



This comparison should be interpreted cautiously due to the fact that *in the case of company III the percentage of disclosures refers to the ratio of the number of requests for users' account data to the number of disclosures regarding those accounts, whereas in the case of the remaining two companies the percentage corresponds to the ratio of the number of requests to the disclosures regarding those requests (irrespective of the fact to what number of accounts they referred). Nevertheless, the differences between the companies are so significant (even between company I and II, which provided analogous data) that they deserve special attention.

On the basis of interviews carried out with the companies and the police we have established three – mutually non-exclusive – hypotheses explaining those situations.

- Differences in the procedures companies use
  The law does not precisely regulate how a request for Internet user data should look, nor what conditions it should meet (compare: analysis on p. 24). Therefore, companies make their own judgments on whether a given request meets formal criteria. As a consequence, it may happen that some of them approve requests which others would consider "filled in incorrectly". As there is no precise regulation, companies must make their own assessments and implement their own procedures.

- Incoherence of the practices on the part of government bodies
  The experience of the companies show that different government bodies apply different standards for data request preparation. Sometimes a company receives a well-justified, complete request – while another time the application needs to be clarified, and this may be reflected in the statistics.

- Differences arising from jurisdiction
  The Internet is a global phenomenon, which means that it does not recognize state borders or jurisdictions and legal orders. As some companies offering services have their seats in foreign countries, the procedures applied in the relations between government authorities and foreign businesses also vary (see: analysis on pp. 21–22).

We make no prior assumptions or judgments on which of the above hypotheses best reflects the actual state of affairs. Nonetheless, we may venture that as long as we know very little about the activities of government bodies towards the companies operating on the Polish market (but being governed by different legal regimes), a fair and reliable comparison of the practices of the companies themselves in the scope of providing user data at the request of public bodies will remain impossible.

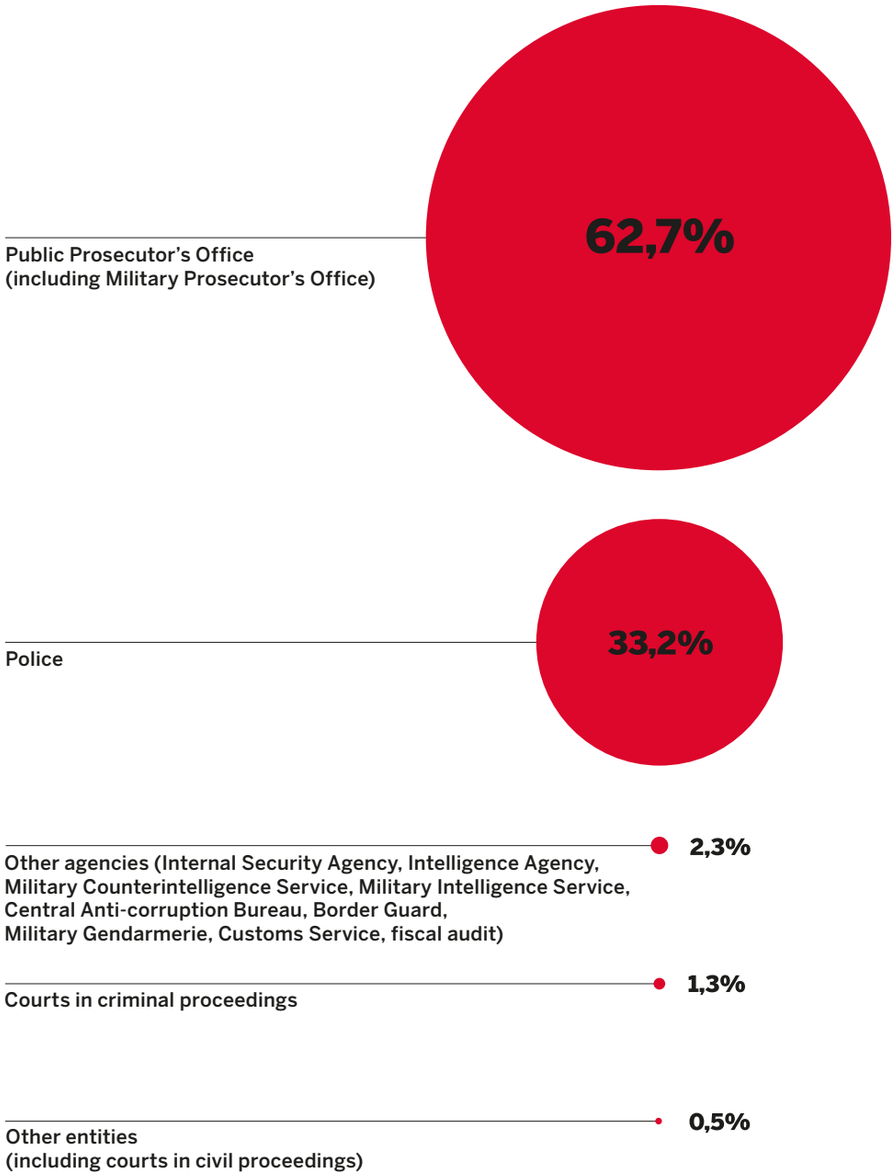
IV. Who makes data requests and why?

A lot more interesting for us than the attempt to examine the scale of requests for Internet users' data was the answer to the question, who, and for what purpose, demands that such data should be disclosed?

On the basis of our talks with companies, we managed to establish which legal grounds public authorities rely upon when requesting the data of service users, which grounds are respected by the companies, and what problems emerge in connection therewith. The conclusions from this analysis are presented in the second part of this study (compare p. 24). Unfortunately, it turned out that none of the firms participating in the pilot study gathers detailed data regarding the legal grounds which the government authorities rely on, and so we cannot determine the share of particular legal grounds in the total number of requests filed.

Nevertheless, we managed to obtain information from three companies regarding which entities request user data and how often they do so. The graph below presents the share of particular authorities in the overall number of demands received by the companies in the period analyzed.

Graph 3: Share of requests made by particular government authorities in the total number of requests filed to Internet service providers in the period 1.01.2012–30.06.2013 (on the basis of data provided by three companies)



The answers given by those companies able to provide us with proper data indicate that the unquestioned leader in terms of requests for Internet user data is the prosecutor's office. The police placed second.

Requests submitted directly by courts are much less frequent, while requests from government authorities – including the Internal Security Agency (ABW) or the Central Anti–corruption Bureau (CBA) – are entirely marginal. At the same time, none of the Polish companies asserted that they are not permitted to disclose certain categories of data requests. In their answers, special services appeared equally often as the police and prosecutor's office. On that basis and that of an analysis of legal provisions, we may submit that Polish companies do not receive data requests from the services on a scale which they would not be able to disclose because of the secrecy obligation by which they are bound.

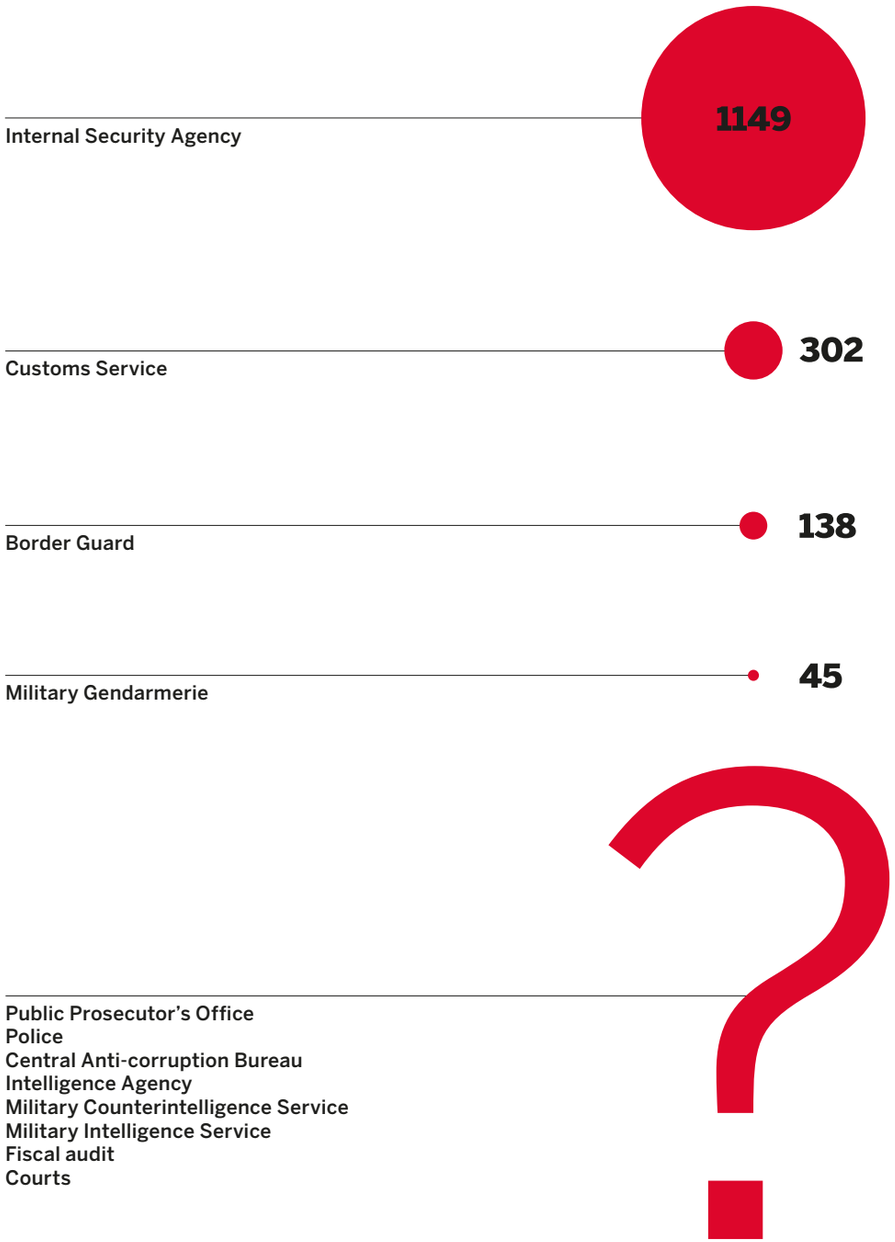
A vast majority of requests for Internet users' data passes through judicial or law enforcement authorities which obtain data for the purposes of criminal proceedings. Assuming that the information provided is reliable, and the government does not make covert requests for data gathered by the companies, there are no premises for assuming that Polish government agencies implement programs of mass surveillance in the scope of collecting information on individuals using Internet services.

Due to the small number of companies which participated in our pilot study, we decided to take a closer look at requests for Internet users' data also on the side of government authorities. For that purpose, we directed analogous questions to the police, the public prosecutor's office, the Agency of Internal Security (ABW), Intelligence Agency (AW), Central Anti–corruption Bureau (CBA), Military Counterintelligence Service (SKW), Military Intelligence Service (SWW), Customs Service (SC), fiscal audit, Border Guard (SG) and Military Gendarmerie (ŻW). Via access to public information we asked these institutions, among other questions, how many citizen data requests – in the same period – they had filed to companies providing Internet services.

Unfortunately, it so happened that it was precisely with these institutions, which (according to the data obtained from the companies) file the most requests, that our motions for access to public information met with resistance. The police informed us that they do not collect data of such kind, so they cannot provide us with any information. The Office of the Prosecutor General answered in a similar manner: as the law does not impose such an obligation on them, at the central level they do not register all the requests directed by particular prosecutor's offices to online service providers. The actual and precise scale of requests generated by these institutions remains, therefore, a great unknown.

However, we managed to obtain data regarding the number of requests filed to Internet service providers from those authorities which theoretically have the most reasons to treat such information as confidential or inaccessible due to other causes. A comparison of their answers is presented below.

Graph 4: Number of requests directed by particular authorized government bodies to Internet service providers in the period 1.01.2012–30.06.2013 (on the basis of data obtained from government bodies)



Of course, without analogous data from the prosecutor's office or the police, it is difficult to assess the scale of requests for data of online service users in Poland. However, on the basis of the collected data, we may submit that the authorities themselves – apart from the police – file few requests. That conclusion is supported not only by the data provided by the companies, but also by the answers of government agencies given via access to public information. On the national level, the number of requests for the data of Internet users which they report is marginal to the entire phenomenon.

V. Context: disclosing telecommunications data

In order to place the discussion on disclosing the data of online service users in a broader context, let's go back to the starting point: the scale of requests for citizens' data which telecommunications operators deal with.

Graph 5: Number of requests directed to telecommunications operators by all authorized government authorities in 2011 and 2012 (on the basis of data collected by the Office of Electronic Communications)

Despite the fact that – as we have repeatedly stressed – raw numbers shed little light on the problems which we are interested in, and hence it is difficult to draw far–reaching conclusions on their basis, the very comparison of the scale of requests for the two data categories does give food for thought.

A comparison of the data published by the Office of Electronic Communications and the data which we obtained from particular government bodies via access to public information indicates that interest in the data generated within telecommunications networks is significantly larger than in the case of online services.

Table: Number of requests directed by particular authorized government bodies in the years 2011–12 (on the basis of data obtained from government bodies)

	To companies providing Internet services	To telecommunications operators
Police	no data	2,894,760
Central Anti-corruption Bureau	no data	195,300
Internal Security Agency	1,299	241,902
Intelligence Agency	no data	———
Military Counterintelligence Service	no data	no data
Military Intelligence Service	no data	———
Border Guard	192	716,726
Military Gendarmerie	32	12,259
Fiscal audit	no data	6,963
Customs Service	268	26
Public Prosecutor's Office	no data	no data
Courts	no data	no data

From the perspective of this analysis, a comparison of the number of telecommunications data requests directed by particular authorized bodies with an analogous set of data concerning requests for Internet users' data seems to be the most interesting. All the more so, as in the case of requests directed by authorities to telecommunications operators we managed to obtain data which were of interest for us from the police (also using access to public information). If we assume that the structure of requests in the case of both types of data – the data of telecommunications subscribers and of online services users – is quite similar, we receive confirmation of the conclusion drawn from the answers of the firms (compare: graph 3): the police is interested in citizens' data to a much larger extent than are the other authorities.

A vast majority of cases of interference with the privacy of Internet service users is connected with criminal proceedings and is taking place under the supervision of judicial authorities, as all data gathered by the police are ultimately put on file or are destroyed as redundant.

The second interesting conclusion regards the vast disproportion between the number of requests made by government authorities to companies providing services by electronic means and the number of those which are directed to telecommunications operators. A comparison of the data seems to confirm what we learned from our conversations with the police: as a principle, law enforcement bodies file demands to companies providing Internet services mostly with regard to the IP number. Establishing the user IP number is usually the first clue in a case, if it concerns using Internet services. If it is at all possible, during the stage of examining the case and gathering evidence, the police and prosecutor's office use more credible and more telling data collected by telecommunications operators (compare: analysis on p. 23). The second factor which may affect the large scale of telecommunications data requests is the possibility of directly making requests for data stored by operators using special interfaces which make it easier and faster to access such data. In the case of requesting Internet services' user data, government bodies do not have such possibilities and each time they have to obtain such data from the relevant provider.

II. Disclosing data: formal principles and practical problems

In this part of the study, we:

- explain the basic principles for collecting data by firms and for making them available to government authorities;
- describe the basic problems and dilemmas faced by companies which disclose data at the request of government bodies;
- diagnose seven key issues which require amending the provisions of current law.

I. What do companies know about their users?

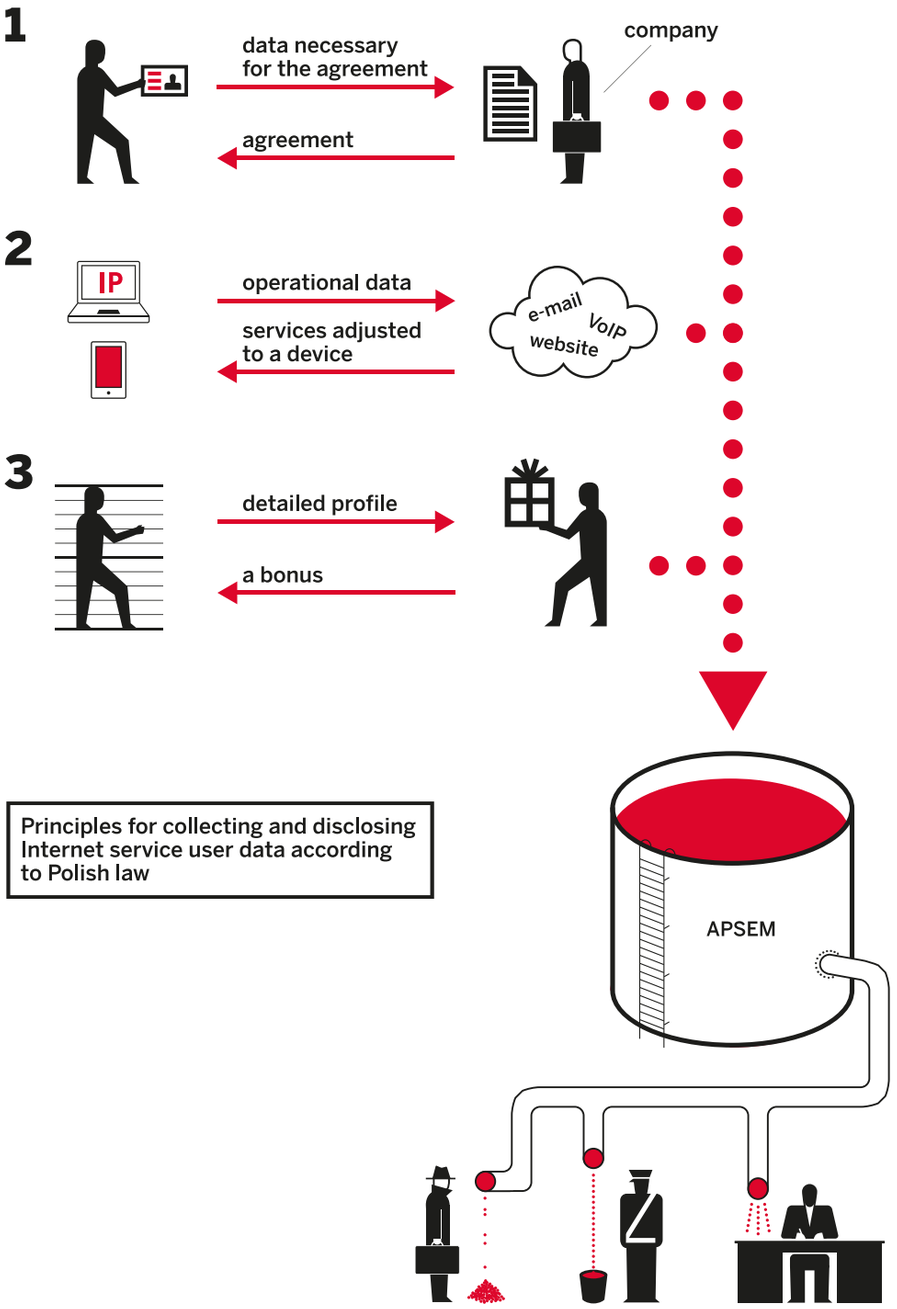
Each movement on the Internet leaves a trace. That trace may be registered by the provider of a service used by a citizen. The more such data a company collects, the more information on citizens may also be obtained by government authorities, as long as they have legal grounds to do so. Therefore, a natural starting point for discussion on the principles for access to the data of Internet services' users should be include a reminder of which type of their data may be processed by the companies themselves.

Essential data

The type of customer data which may be processed by a Polish company providing online services is strictly regulated by law. As a principle, it is the only essential information required to provide and bill the service in question.

This category includes:

- personal data necessary to enter into the agreement: e.g., name and surname, PESEL (national identification number), e-mail address (compare: infographic – 1);
- "operational" data that is necessary to "adjust" a given service to the user's hardware and software: e.g., IP number, information on browser settings and installed software (compare: infographic – 2).



Principles for collecting and disclosing Internet service user data according to Polish law

Storing the content of correspondence may also be essential for the purposes of providing a given service, if that is what the customer expects – e.g., in the framework of electronic mail services that use data hosting on a virtual server. Of course, this does not at all mean that the company has the right to read our e-mails and use their content for purposes other than those arising directly from the agreement.

Another example of personal data collected by companies may be the address to which an online shop delivers the goods purchased. However, the principle is still the same – the company has to have a clear reason arising from the specific features of its operation to process that information.

The principles for collecting and storing customer data in Poland are regulated by the Act on Providing Services by Electronic Means and the Act on Personal Data Protection (APSEM). However, these provisions may be disregarded by those companies which do not fall within Polish jurisdiction, even if they operate on the Polish market.

Additional data

It may happen that a company wants to collect data which are not essential for the provision of a service ordered by the user – e.g., for the purposes more tailored advertisements or improving service quality (compare: infographic – 3). In this context, such information as activity history in the Internet service, the detailed profile of a user, or information on contacts with other users may be very attractive.

If a company wants to process personal data which are not essential to provide the services, it may do so only with the consent of the user. In practice this means that it should inform each user regarding which additional piece of information about him or her it wants to collect and then ask whether he or she accepts such terms and conditions of service provision.

Regulations which arise from the Act on Providing Services by Electronic Means and the Act on Personal Data Protection do not have to be adhered to by those companies which fall outside Polish jurisdiction (companies registered outside Poland and not processing data on the territory of Poland). In their case, the principles for user data collecting and processing are specified by the law of the country of origin.

II. Principles for disclosing data to government authorities

The information necessary from the perspective of companies, as well as that which online services users give them voluntarily, may prove to be equally attractive from the point of view of the state. The most frequent reason for such interest is that of combating crime, and more specifically, the need to gather evidence in an investigation against a given person. The principles on which government authorities may use data collected by companies are also provided for by the law.

On the one hand, the Act on Providing Services by Electronic Means imposes on all companies providing such services the obligation to "disclose information on the processed data to government authorities for the purposes of proceedings conducted by them" (Article 18 Section 6 of APSEM). Similarly to the limitations concerning the collecting and processing of personal data, the obligations arising from that act refer

only to those companies which fall within the Polish jurisdiction. Foreign businesses adhere to such regulations as are specified by the law of the country of their incorporation.

However, the obligations of companies arising from the Act on Providing Services by Electronic Means are only one side of the coin. For the law gives to particular government bodies clear authority on the basis of which they may demand that companies provide them with the personal data of Internet service users. In relation to those bodies which hold executive authority, all the companies operating on the territory of Poland are equal. Foreign companies must also abide by the decisions of the court and the prosecutor or requests directed by the police on the basis of their legal competence.

Pursuant to the Polish Code of Criminal Proceedings (Articles 218 and 236a) the prosecutor and the court have the right to demand data when they are of significance to specific proceedings.

On the other hand, under the Police Act (Article 20 Section 2a) the police may collect and process the personal data of suspects without their knowledge and consent. An analogous solution is provided for in the so–called competence acts, regulating the operation of specific authorities (among others, the Internal Security Agency, Central Anti–corruption Bureau, fiscal audit, and the Customs Service). The provisions regulating the functioning of the police and other authorities treat only certain types of data differently (e.g., banking or insurance data), whereas they do not provide for any separate rules of conduct in relation to the data of Internet service users. Hence the conclusion that the authorities may demand access to such data (as a category of personal data) on the basis of general provisions concerning personal data collection.

Polish regulations do not allow for the free access of the government to databases in which companies store the data of Internet users. The prosecutor's office, the police, and other bodies may only obtain information regarding specific individuals. They must always present an appropriate request or decision that clearly spells out its legal grounds.

Various standards for protection of electronic correspondence

Under Polish law the standards for correspondence protection are not uniform. They depend on the status of the company storing it. Telecommunications operators are bound by so-called telecommunications secrecy. In practice, this means that the operator cannot familiarize itself with the content of stored correspondence (e.g., text messages – SMS) or listen in on phone calls in progress; nor can it allow other entities to do so, unless telecommunications secrecy is overruled by virtue of the decision of a criminal court. The provisions regulating the principles for providing Internet services – including electronic mail – do not provide for any analogous protection. Therefore, telecommunications secrecy does not protect correspondence stored by companies providing services by electronic means.

What are the practical consequences of such a state of affairs? Fortunately, the police and other bodies, although they are not limited by telecommunications secrecy, may not freely access the content of correspondence; their competence provisions in such situations impose an extraordinary course, regardless of who stores the correspondence. However, it happens that civil courts which treat all information held by companies as "documents" may demand that an online service provider disclose the correspondence of its users. When doing so, they refer to the provisions of the Polish Code of Civil Proceedings, allowing the courts to have access to documents for the purposes of evidence collection. Although the companies do not store the correspondence of their users and do not hold "documents" of that type, a refusal to perform the decision of a civil court may entail the necessity to pay a fine.

The citizen is not always aware that he or she had been "checked"

Do citizens know who requests data pertaining to them, and when? That depends on who makes such a demand. Courts and prosecutors acting on the basis of the Polish Code of Criminal Proceedings must issue a decision which is delivered not only to the company, but also to the person to which it pertains. Regulations allow the courts and the prosecutor to adjourn the delivery of such a decision in the interest of the proceedings, but the obligation to inform the citizen that he had been "checked" does not disappear. Entirely different rules apply in pre–trial proceedings: neither the police nor public authorities have to inform the person whose data they had used in the framework of operational activities. That knowledge is possessed only by the companies to which the authorities direct their requests.

Information most frequently sought: IP address

Our talks with practitioners have shown us that out of the entire catalogue of available data, the most interesting type of data for the police and the prosecutor's office is the IP number. As opposed to the particulars which users themselves give to Internet services providers, this information is difficult to change or falsify. On the basis of the IP number, law enforcement agencies are able to further specify, e.g., the address or name of the suspect. Due to the greater credibility of data held by telecommunications operators, they usually receive further requests (which may be referred to as "belaboring the topic"). This arises, among other reasons, from the fact that in order to enter into certain types of contracts with a telecommunications operator it is necessary to present a document.

III. Vague procedures and legal grounds

The law does not precisely specify the elements which a data request addressed by government authorities to a private company should contain. This causes interpretative doubts which the companies have to resolve according to their own judgment and at their own risk.

In order to obtain information about a given Internet service user, government agencies and bodies always have to refer to a specific legal basis. One of the most frequently applied legal grounds is that of the very laconic Article 18 Section 6 of APSEM, which reads: "The service provider shall provide information on the data referred to in Sections 1–5 to government authorities for the purposes of proceedings conducted by them". And it is around this provision that a unique interpretation dispute is being waged.

The above provision imposes on firms an obligation to provide data at the request of "government authorities", but does not specify which entities fall into this category (in practice, doubt arose over whether, for instance, a medical chamber or a forester are also government bodies authorized to collect data). However, in the opinion of the authorities themselves – including the police – Article 18 Section 6 of APSEM is quite precise and does not require amendment. According to the information given

to us by the police, on the basis of that very provision (and not the Police Act) the Chief Commander of the Police authorized a group of officers to collect data from companies providing Internet services, in particular to verify IP numbers.

Certain companies differ in their view on this issue, claiming that in order to disclose data they need a clear legal basis applied by the requesting authority. **Our conversations with the firms have shown that the practice varies depending on the company: some of them respond to requests based solely on Article 18 Section 6 of APSEM, others additionally demand a clarification of legal grounds arising from the so–called competence act** (regulating the principles for the operation of the police and other agencies).

But this is not the end of the interpretative doubts. The law does not precisely specify those elements which a data request filed by government authorities to a private company should contain (e.g., specifying the reference number of the case in which the proceedings are pending; officer's signature; seal of the institution). Moreover, it is not defined how a company should act when it receives an incomplete request (return it with a request for supplementation, or perhaps refuse to disclose data?), or how to act in urgent cases, e.g., mortal danger, when there is no time for excessive formalities. In effect, the decision on whether to ask government authorities to make additional clarifications or – due to justified circumstances – simply process a request, depends solely on the judgment of the given company.

Furthermore, the applicable provisions do not precisely specify how government authorities may direct to Internet service providers requests for data of their users. Also in this sphere does practice – both of the companies and government bodies – differ. Smaller companies still receive requests from government authorities sent by traditional postal services. In contacts with larger businesses which can afford to implement secure electronic communication channels this form of communication is also employed. The police confirms that it has established secure, encrypted connections with certain firms precisely for the purposes of a more efficient submission of data requests. However, direct access to databases, or an interface allowing for individual data collection, is out of the question – although in urgent cases (e.g., a threat to life) it may happen that answers are given to requests filed over the telephone.

Disputes regarding cost reimbursement

The necessity to respond to requests made by government bodies generates certain costs. They are connected with collecting information sought by a given authority, printing out hundreds of extracts, and sending them by traditional mail. The law does not precisely specify whether companies are entitled to a refund of the costs incurred in this process. They apply various methods of coping with this problem: some of them collect charges for disclosing data, others do this at their own expense. It also happens that firms seek cost reimbursement in a court of law.

Abuses related to data access

There are known cases of notifying the public prosecutor's office of a crime of copyright infringement by associations dealing with copyright protection only to reach the personal data of alleged "pirates" with the help of law enforcement bodies. Having obtained such information, such associations or their representatives file a demand for payment for a breach of copyright directly to the user, which may be treated as a form of blackmail. Such activities exploit the mechanisms of the criminal process and the government authorities in a civil dispute, thus they constitute an abuse of the law.

IV. Control mechanisms

Polish law does not provide for a uniform mechanism for controlling the activities of government bodies when it comes to using the data of Internet service users or other categories of personal data. Inspection by an independent body – e.g., a court – is conducted principally only in the case of certain types of proceedings; in other cases there is no such control.

In criminal proceedings the law provides for several independent control mechanisms. Primarily, the court or the prosecutor decide on the provision of data, but always under supervision of the court – that is, an independent body. Additionally, the decision on requesting personal data is delivered to the person concerned. Such delivery may be adjourned until the end of the proceedings, if it is necessary with regard to the interest of the case. However, the very obligation to notify that the data was used in the case does not disappear. What is more, the person to whom such a decision pertains is authorized to file a complaint which is examined by the court.

There are no analogous "safety valves" and mechanisms of control over requesting Internet service users' data during the stage of operational activities conducted, e.g., to combat crime or conduct undercover surveillance of criminal structures. Such activities are confidential by their very nature. Information that the bodies were interested in the data of an online service user while conducting operational activities will reach that person only when criminal proceedings are instituted. If the collected data do not provide enough grounds to do so, the information on the data having been gathered by the police and the authorities will not reach the user.

During the stage of operational activities, the police and other authorities may request data of Internet service users without external control exerted by the prosecutor's office or the court. What is more, special services are not controlled even by the Inspector General for Personal Data Protection. However, data requests pass through the system of internal control. The information which we obtained from the police shows that no officer may file a data request on his or her own; to do so, they need the consent from their superior. However, that consent may take the form of a permanent authorization.

Statistics and reporting

Companies providing online services are not obliged to inform anyone on how often government bodies request the data of their users and how many of these requests are ultimately processed. The obligation to provide information of this type is nevertheless imposed on telecommunications operators, which (within the meaning of the binding provisions) are entities of a different type. Data originating from them are gathered by the Office of Electronic Communications and – as it turns out – the transparency of these statistics does not make it difficult for prosecuting or judicial authorities to perform their work. On the other hand, however, the best source of such statistics are undoubtedly government bodies and it is mainly them that should collect the information on requests directed to private entities and make it available to the general public.

V. Summary: key issues

Our analysis of the legal provisions and information collected from firms and other entities processing Internet user data gave us grounds to describe systemic issues connected with providing data at the request of government authorities. We have covered them in detail above, whereas at this point we would like to underline them and draw a summary.

Issue number one: it is impossible to assess the scale of requests

Certain data are lacking that would illustrate the scale of requesting the data of Internet service users. Since companies providing services by electronic means are not obliged to keep a register of requests filed to them by government bodies and publish reports on that subject, only some of them do so – on their own initiative and according to their own principles. What is worse, such an obligation is not imposed on the government bodies either, in consequence of which only some of them have appropriate data. As a result, we do not know how many Internet user data requests are made, to what they specifically refer, who files them, and how many of them have been processed. Therefore, it is all the more difficult to evaluate whether or not, for instance, the possibility to access Internet service user data actually has any influence on combating crime or on the operational work of government agencies.

Issue number two:
companies must resolve serious interpretation problems on their own

The law does not precisely lay down which formal criteria a data request should meet and in what way it should be delivered to a company (e.g., whether or not electronic form is admissible). This uncertainty is further aggravated by interpretation problems connected with the key basis for requesting data processed by online service providers: Article 18 Section 6 of APSEM. In practice, the entire burden of evaluating whether or not a given data request has been prepared properly and whether the legal basis to which the requesting entity refers is sufficient – is on the private entrepreneur. As a consequence, it is difficult to talk about a coherent standard for protecting user privacy – each company makes such an assessment at its own discretion. The lack of precise provisions also makes it difficult to develop a uniform method of data collection for statistical purposes – e.g., it is not known how to count a request which contains queries regarding many users. Doubts of such kind arise exponentially.

Issue number three: no control over data collection by the authorities

There is no external supervision and no independent mechanisms for verifying whether the services (e.g., Internal Security Agency or Central Anti-corruption Bureau) exploit Internet user data in accordance with the binding law. That problem has many times been highlighted by the Ombudsman, whereas the Supreme Audit Office in its recent report notid that no authority in Poland controls whether the services indeed operate within the limits and on the basis of the provisions of law. This issue also concerns e.g., the exploitation of online service user data. Where personal data are involved, the problem of a lack of supervision over the operation of the services is deepened by the fact that citizens themselves have no possibility to verify whether public authorities have requested companies to disclose their particulars. For the purposes of comparison: in court proceedings, the defendant has the right to information that his or her data were taken for the purposes of the case and may even file a complaint in connection with this.

Issue number four:
various procedures for data disclosure remain in force at companies

On the one hand, Polish law provides specific limitations for companies when it comes to the possibility to gather data on Internet users – on the other, it imposes on those same companies the obligation to disclose personal data on the demand of authorized bodies. Not all of these rules apply to foreign companies: although they have to adhere to criminal law provisions to the same extent and cooperate with the courts or the police, they are not subject to the obligations arising from the Act on Providing Services by Electronic Means. In practice, they have similar obligations towards the state, but they operate on the basis of different procedures. This discrepancy between the rules – irrespective of which of them in practice proves better with regard to user data protection – leads to a situation in which we are unable to reliably compare the practices of all companies operating on the Polish market.

Issue number five:
lack of clear regulations concerning reimbursement of the costs of request processing

The lack of clear regulations concerning reimbursement of the costs of processing requests from government bodies gives rise to a situation in which companies must face an additional problem: either accept that additional burden or demand that their costs be refunded in a court of law. In the case of collecting telecommunications data (from telecommunications operators) the law resolves the cost issue in a manner unfavorable to the operators: the provisions clearly specify that data shall be provided free of charge. There is no analogous provision in the case of companies rendering online services. In effect, interpretation disputes arise very often between the companies and government authorities. As a principle, courts acknowledge that companies have a point here, and confirm their right to demand a refund of costs incurred – yet the vagueness of the existing provisions generates additional expenses (of lawsuits) and consumes time.

Issue number six:
non-uniform standards for protection of electronic mail and telecommunications data

In Polish law, the standard for correspondence protection depends on the status of the company storing it. Correspondence (e.g., text messages – SMS) sent via telecommunications operators is protected by telecommunications secrecy. Electronic correspondence (e.g., e-mails) stored by companies providing services by electronic means is not granted analogous protection. Therefore, in practice it happens that civil courts, which treat all information held by companies as "documents", demand from online service providers that they disclose the correspondence of their customers. They would not be able to make a similar request to a telecommunications operator.

Issue number seven:
instrumental use of criminal proceedings to "dig up" personal data

The experience of companies confirms that it may happen that entities dealing with copyright protection use criminal proceedings and the competences of the prosecutor's office in an instrumental manner. Initiating criminal proceedings (by filing a notification on a crime committed) has one goal: to specify the personal data of a user who allegedly breached copyrights. Such data (put on file) are then used to "seek rights" on one's own account. Most often such a user receives a threatening letter with a demand of payment. This is an unethical practice, deeply interfering with the rights of citizens.

***

Data on Internet service users are just one of many types of personal data processed by private businesses to which public entities may gain access. The provisions regulating the functioning of the police and other bodies treat only certain types of data differently (e.g., banking or insurance data), while all the other types are collected according to the same principles. Therefore, some of the issues raised above are of a systemic nature: they do not concern only the police and other authorities requesting data of Internet service users. The above refers mostly to the inability to assess the scale of data requests and to the lack of control over collecting data by public authorities.

KEY PARTICIPANTS OF THE PROJECT – ACKNOWLEDGEMENTS

We would like to thank the following companies: **Interia.pl**, **Onet**, and **Agora** for devoting their time to think over the answers they gave us, as well as their full readiness to talk about how the provisions imposing the obligation to disclose user data function in practice. Their experience proved to be especially significant for us, as these companies operate within the framework of our domestic law. It was also important that **Google** joined the project – a company which for several years now has been publishing transparency reports – as its experience is representative for foreign businesses. We also appreciate the willingness of Facebook to join the project. **Facebook** published its first transparency report this year and we hope that this will mark the beginning of a permanent good practice. Unfortunately, due to the insufficient scope of disclosed data, we were unable to include their answers within this report.

The work on the concept was a suprasectorial enterprise. We were given assistance from the **Ministry of Administration and Digitalization** – indeed, our first working meeting was held under its auspices, and Minister Michał Boni publicly underlined the necessity to examine the scale of interest of government authorities in the data of users of Internet services. We were also offered pro bono support from the **Bird & Bird** law firm, which acted as an intermediary in transferring data between the companies and Panoptykon Foundation. The law firm pseudonymized the completed surveys, owing to which we cannot ascribe the answers to particular companies.

Panoptykon Foundation | panoptykon.org

PANOPTYKON FOUNDATION

Authors
Katarzyna Szymielewicz, Małgorzata Szumańska

In cooperation with
Wojciech Klicki, Anna Mazgal, Anna Walkowiak

Translation
Eliza Jakubiak

Graphic design
Filip Zagórski / filipzagorski.com

Warsaw 2013

This publication contains conclusions from the project implemented by Panoptykon Foundation with the financial support of Google.