Anonymous ePetitions – Another Step Towards eDemocracy

Hannah Obersteller

Anonymous ePetitions – Another Step towards eDemocracy

Hannah Obersteller

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany

hobersteller@datenschutzzentrum.de

Abstract. This paper addresses the possibility to implement an online petition platform which allows citizens to petition the public authorities anonymously. The advantages and possible obstacles of anonymity are discussed. We focus on the legal admissibility of anonymous petitions in Europe and Germany and conclude that all related legal requirements could be met by implementing Privacy-enhancing Attribute-based Credentials.

Keywords: Privacy · Privacy-ABCs · eDemocracy · ePetitions · Anonymity

1 Introduction[1]

A petition is a democratic instrument that allows – in general – the members of a country, a state or other kinds of community to introduce their concerns to the political decision-makers and thereby influence the political dialogue. The petition offers the possibility to raise an issue and obliges the democratically elected representatives to address this issue. E.g., the German constitution (Grundgesetz; abbr.: GG) guarantees everyone to petition the public authorities (Art. 17 GG). Art. 45c GG determines that a committee of petitions shall be established. This text, however, will focus on petitions to parliaments.

In the last few years, citizens have been provided an increasing number of ways to get into contact with public administrations. In the context of the so-called "e-government movement" many administrative issues now can be performed by sending e-mails or using online services. The current German and European legislation allows for the possibility to file petitions online. Advantages of information and communication technologies, as e.g. being independent from time and location (cf. [1], pp. 357, 358), support these methods of e-participation. This paper focuses on the advancement and improvement of the existing systems with regard to the protection of the citizens' right to privacy.

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

For instance, in 2005 the German federal Parliament (Bundestag) introduced the possibility to file petitions online. At the same time, a new form of petitions was introduced: public petitions. A public petition is published on the Internet, i.e. on the website of the Bundestag, and can be signed by other people during four weeks. The Directive on public petitions which concretizes the Rules of Procedure of the Bundestag (RoP BT) determines that the petitioner has to indicate his name, permanent address and e-mail address. If the petition is meant to be a public petition, the name and contact address of the petitioner will be published with the petition text. (According to the "Help" section of the Bundestag's website, only the name of the petitioner is published [2].)

While already the fact that a petitioner has to identify herself by revealing her name and full address to the petition committee, as petition recipient, is to be considered as critical, the publication online is an even stronger intrusion in the petitioner's privacy. The employment of Privacy-enhancing Attribute-based Credentials could be a solution. This technology allows petitioners (and signees) to stay completely anonymous while at the same time it is guaranteed that they are legitimized and do not sign a petition several times when only one signature per person is allowed. Note that current systems do not prevent multiple signing if someone has more than one e-mail address.

The objective of this paper is to discuss how far it is possible to introduce a system which allows submitting a petition not only online but at the same time anonymously, i.e. without disclosing one's name and address to the respective petition committees. The reasoning is based on European legislation. In addition, German legislation is analyzed for input on the Member State level. Furthermore, it is debated how far staying anonymous is possible when submitting a simple petition or a petition that is to be signed by other citizens and, finally, if signees can stay anonymous in the latter case, too.

The text is organized as follows: First, key terms are defined in Section 2. Section 3 provides an overview of the current legal framework concerning anonymous use of online services and petitions on European and German level. Obstacles to overcome are discussed in Section 4. Finally, it is concluded that anonymous ePetitions would support eDemocracy.

2 Definitions

2.1 Petitions and "ePetitions"

Traditionally, a petition is submitted as a document, written on paper, signed in manuscript by the petitioner(s). Nowadays, public authorities increasingly allow the submission via online form. The general process of a petition stays the same and is as follows:

1. A citizen (the petitioner) formulates her concern in writing. Often a (online) form is provided. Inter alia she has to provide her full name and address, in order to allow the public authority to identify the petitioner and contact her by post.

2. The public authority that receives the petition is obliged to examine the admissibility of the petition (compliance with the respective procedural requirements, e.g. competence of the public authority on the petition subject). Mostly, parliaments have established petition committees that process the incoming petitions.
3. If the petition is admissible, the petition committee is obliged to decide on the petition. The exact procedure (oral proceedings/summons of the petitioner or just a written decision with or without grounds) depends on the individual case. But the petition committee is obliged to reply to the petition and to send the petitioner a final reply.

There are different possible understandings of the term "electronic petition" (or: "ePetition"): It can be defined as the submission of a petition to the addressee electronically. In this case the only aspect different for ePetitions compared to "traditional" petitions (in writing) is the modernized way of filing. The actual petitions process would not have to change ([3], p. 11). Another definition of "ePetition" could be "a petition that is published on the Internet". It does not necessarily have to be submitted electronically, but the further petitions process would happen online ([3], p. 11). Within this latter case one can make another distinction between a passive and an active way of use. A passive way of use would be that the petition (and eventually the petition notice) is simply made visible online. An active way of use would mean that an electronic petition system is set up, which especially enables people to file, and others to sign the petition online ([3], p. 12).

In the following "ePetition" will be understood as a petition filed (and possibly published) online and "public ePetition" will be understood as a petition filed online and published on the Internet that can be signed by other people (signees) online. This understanding of "public ePetition" corresponds to the definition of "public petition" laid down in the Rules of Procedure of the Bundestag concerning petitions (see 2 (4) RoP BT). On the European level, only (simple) ePetitions exist. Both kinds of ePetitions can be filed by several petitioners together.

2.2 Privacy-enhancing Attribute-based Credentials

Privacy-enhancing Attribute-based Credentials (Privacy-ABCs) give the user control over which, and how much personal information she reveals. They allow authentication towards an online service provider without identification. In a Privacy-ABC system the following entities are mandatory: issuer, user and verifier.

The issuer knows and can vouch for attribute values of the user. The issuer issues a Privacy-ABC credential containing those attributes to the user. The user receives the credential. Whenever the user wishes to authenticate, the credential on her device is combined with her individual secret key that only she possesses. The result is called a token. The user now can use this token to provide proof of certain attributes towards a third party – normally a service provider – which is called the verifier. The verifier offers a certain online service and usually has a presentation policy that determines which information is demanded to access the service. If e.g. the verifier is an information portal of town X that offers the possibility to ask questions on community issues to the inhabitants of town X, the user will only have to prove that she is an

inhabitant of town X. Further information that may be contained in the user's credential, like e.g. her name and exact address, she can strip off. If the information stored in the token that the user provides meets the requirements of the verifier's presentation policy, the user is allowed to access the desired service. As a result, the user does not have to reveal more information than absolutely needed to make use of a certain online service. This supports the data minimization principle (see also Section 4.2).

Besides the above mentioned mandatory entities, a Privacy-ABC system can additionally comprise further entities: If full anonymity is not desired, ways for conditional identification can be allowed. This would be done by adding the "inspection feature"." This means, in order to allow the revealing of the user's identity if necessary, an independent "inspection entity" can be employed. The "inspector" is allowed and enabled to identify the user only if predefined conditions are fulfilled. Those "inspection grounds" could, for instance, allow the revealing the identity of a user in case of misuse or infringement of third parties' rights. They have to be made known to the user in advance. Furthermore, it may become necessary to revoke a credential, e.g. if the user's attributes, stored in this credential, have changed. For this purpose, a "revocation authority" can be established. The inspection and revocation processes have been discussed in detail in [4].

In principle, the user can be enabled to act completely anonymously. However, while Privacy-ABCs allow anonymous authentication, the implementation has to be considered in detail as certain circumstances, such as the specific value of revealed attributes, tracking measures (cookies etc.) and IP addresses, may hinder this capability. An illustrative example of how a Privacy-ABC-based petition system which allows complete anonymity could be implemented was already given and discussed in the past in [5].

2.3 Anonymity

According to the European Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; respectively its national implementing laws), a data subject is considered as anonymous if she is not or no longer identified or identifiable. "(…) To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (…)." (European Data Protection Directive; Recital 26; omissions by the author; cf. the draft General Data Protection Regulation, Recital 23) "Identification" does not only mean that it is possible to retrieve a data subject's name and/or address, but also identifiability by singling out, linkability and interference ([6], p. 10).

The document referenced in [6] also explains in detail different ways of anonymization. In general, identifiability of a single individual depends to a large extent on the distinguishability of this person within a set of individuals. The larger the set of people sharing the same attributes values is, the more unlikely is the identification of an individual. So ideally, an anonymous ePetition system has to avoid storing information that might allow the data controller – or an external attacker – to directly iden-

tify the users or link the information with other databases and use the retrieved information in connection, in order to identify the users ([7], p.42).

Privacy-ABCs systems provide a possible solution, since the service provider – in this case the provider of the ePetition platform – does not receive more data than absolutely necessary and, consequently, cannot store them. In most cases, e.g., it is sufficient to prove that one is citizen of a certain state (or maybe region) to participate in a certain ePetition. Still, Privacy-ABCs allow to make sure that a citizen signs a petition not more often than once. (See also Section 4.3. For more details on the technical solution please refer to [8], pp. 128 et sqq.)

However, in case of complete anonymity the European Data Protection Directive is not applicable, since it only regulates the handling of identifying data (Recital 26 Dir. EC/95/46; [6], p. 5). From a legal point of view, anonymity is not given if the user is not identified from the outset but still identifiable ([6], p. 6), i.e. her identity can be revealed. In a Privacy-ABC system which enables the inspection feature, the credentials issued to the user are "inspectable". If the inspection grounds are fulfilled, the inspector is (technically) enabled to reveal the user's identity.

Assuming that an ePetition system will not be accepted by the responsible public authorities if identification is absolutely excluded, it would probably be more accurate to speak of "anonymous or pseudonymous" ePetitions when discussing the possibility of employing Privacy-ABCs with or without the inspection feature for this purpose. But since anonymity (in the legal sense) is technically possible, it seems acceptable to focus on this goal. Pseudonymity, however, means that the linkability of a dataset with the original identity of an individual is reduced ([6], p. 20).

3 Legislation

Since 1992, the right to petition the European Parliament is laid down in the European legal framework. Prior to that, it was recognized by customary law and mentioned in the Rules of Procedure of the European Parliament ([9], p. 344).

Today, it is guaranteed by the Charter of Fundamental Rights of the European Union (CFREU), the Treaty in the Functioning of the European Union (TFEU) and in many constitutions of the EU Member States ([9], p. 344, fn. 1385). As mentioned initially, in Germany it is constitutionally guaranteed in Art. 17 GG. The competence of the respective public authorities depends on the subject of the petition. For instance, the Bundestag is not responsible for the educational policy of the German federal State Schleswig-Holstein. If a petitioner files a petition concerning the inadequate curricula of public schools in Schleswig-Holstein, the Bundestag's petition committee will inform the petitioner that her petition was rejected as inadmissible.

3.1 Anonymity

If the operator wishes to store identifying data of the user (e.g. the IP address), he needs a legal permission. As the IP address commonly is regarded as personal data ([10], p. 16), the European Data Protection Directive is applicable. This means, data

may only be collected for specified, explicit and legitimate purposes. Under the current German legislation there is no general legal permission (or even obligation) for website operators to know or to store identifying personal data of their users. While telecommunication providers in Germany are obliged to collect identifying personal data such as name, permanent address, date of birth etc. from their customers (cf. § 111 Telecommunications Act; abbr.: TKG), this does not apply to website operators. The latter (usually) are not telecommunication providers.

A "telecommunication provider" is a natural or legal person offering telecommunication services. "Telecommunication services" are offers of telecommunications, including transmission line offers to broadcasting networks, usually for a consideration (§ 3 Nr. 18 TKG). "Telecommunications" means the technical process of sending, transmitting and receiving any kind of message in the form of signs, voice, images or sounds by means of telecommunication systems (§ 3 Nr. 16 TKG).

Provided that the operator of an online petition platform does not run an own telecommunication network, he does not meet this definition as he does not offer access to a telecommunication network. To website operators the German Telemediengesetz (Telemedia Act; abbr.: TMG) applies. Both the TKG and the TMG serve to implement European legislation on national German level; i.e. the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) amended by the Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009. The TMG itself does not oblige (or allow) the website operator to store user data. The responsibility and liability of website operators depend on his role. A website operator who is just running and maintaining the website, but does not provide own editorial contributions is regarded as host provider (Art. 14 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; "Directive on electronic commerce"). Concerning the content a petitioner publishes at the petition platform, the Bundestag (as website operator) does not provide own contributions online. A moderator will just delete user content which is not compliant to the terms of use [11]. Hence, the Bundestag is to be treated as a host provider in this regard. In consequence, a right to store the user's personal data for own business purposes because this is necessary to safeguard its legitimate interests (according to § 28 (1) Nr. 2 Federal German Data Protection Act; abbr.: BDSG) cannot be derived, as a host provider is not responsible for user content. Otherwise the legitimate interest could be e.g. evidence purposes or own legal actions in case of legal proceedings against the website operator due to content published by a user [12]. The host provider is just required to make sure that such content is deleted, respectively not accessible anymore (§ 10 TMG).

The website operator of an Internet forum is not required to provide an individual with personal data of one of the users, even if this user has published content which violates the rights of personality of this individual [13]. In turn, the operator has to provide the prosecution authorities with stored personal data in cases of suspicion of serious criminal offences committed by the user. But if no identifying data is stored,

the website operator cannot provide the authorities with such data. Currently, there is no German data retention law: In 2010 the German Constitutional Court (Bundesverfassungsgericht) ruled that the German transposition law to the European Directive on retention of personal data (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) was void.

This may be regarded as an unintended gap, since the technical possibility of complete anonymity just was not considered. But de facto there is not even a rule of law which regulates a comparable issue and therefore could be applied by analogy.

3.2 Legal Requirements on Petitions

The right to petition grants that the petition recipient examines the petition content. If the petition recipient comes to the conclusion that the petition is not admissible, the right to petition further grants that the petitioner shall be informed about this fact and the reason for the inadmissibility. Reason for this is to allow the petitioner to make a decision on whether she wants to appeal the decision and to allow a judge to review the grounds for lawfulness. Insofar, the right to petition is identical on European and national German level ([14], [15], [16]). However, as for the national German level, the German constitutional court ruled that the petition committee is not obliged to provide the petitioner (of an admissible petition) with a statement of grounds for its decision. Once a petitioner got a reply for the purpose of notifying the decision on her petition, she has no right to get another reply if she petitions to the same authority for the same reasons again [14].

Under the current legislation – leaving aside the subordinate Rules of Procedure, which could be attached autonomously by the respective parliaments or petition committees themselves – it is possible to implement an anonymous ePetition system.

The current Rules of Procedure of both the European Parliament and the Bundestag determine that the petitioner has to identify herself towards the petition committees. Staying anonymous or using a pseudonym towards the petition committee is not allowed.

However, the Rules of Procedure stem from the fact that the treatment of petitions is left to the discretion of the public authorities, as long as the minimum conditions are fulfilled ([17], marginal 10). The parliaments could change their respective Rules of Procedure and allow anonymous ePetitions as long as compliance with the "minimum conditions" is assured.

European Union. The European legislation allows every citizen of the European Union and any natural or legal person residing or having its registered office in a Member State to petition the European Parliament alone or jointly with others (Art. 44 CFREU, Art. 227 TFEU). Art. 227 TFEU limits the scope to matters which come within the Union's field of activity and affect the petitioner directly. Petitions will be addressed by the Petition Committee of the European Parliament. According to the

Rules of Procedure of the European Parliament (8th parliamentary term, July 2014; abbr.: RoP EP), the Petition Committee is one of the standing committees which are to be set up by the European Parliament (196 RoP EP; Annex VI (XX)).

It is possible to file petitions via an online form (or by post). It is not possible to file a petition as public ePetition, but – as Art. 227 TFEU provides – to file petitions together with as many other petitioners as desired. The petitioner has to indicate her name, permanent address and nationality. If the petition is published online, the name of the petitioner may be published with the petition's content (215 (9) RoP EP). Basically, all registered petitions will be made public documents and may be published by the European Parliament (215 (9) RoP EP). Nevertheless, the European Parliament has itself undertaken to respect the privacy interests of petitioners to such degree as Rule 215 also stipulates the mandatory non-disclosure of the petitioner's name (Rule 215 (10) RoP EP) or the possible treatment of the petition (the content) as confidential (Rule 215 (11) RoP EP) if the petitioner clearly requests this when filing the petition.

In contrast to the German constitution, neither the CFREU, nor the TFEU states clearly that a petition has to be filed in writing. Still, the RoP EP anticipate that petitions are "written" (c.f. 215 (5) RoP EP: "Petitions must be written in an official language of the European Union."), which of course does not necessarily mean in a traditional – meant as "on paper" – way. However, in accordance with the Bundestag, the European Parliament decided to give potential petitioners the ability to file petitions online. But all subsequent communication will happen by post. As this communication could be done electronically as well, there is no absolute hindrance for anonymous ePetitions.

Germany. As stated in the introduction, on the German federal level the right to petition the Bundestag (and other public authorities) is guaranteed in Art. 17 GG. Art. 45c GG determines that a petition committee is to be appointed by the Bundestag. All powers conferred to the petition committee of the Bundestag are regulated by federal law (Gesetz über die Befugnisse des Petitionsausschusses). All details concerning action taken on petitions are laid down in the petition committee's Rules of Procedure (introduced on the basis of § 110 of the Bundestag's Rules of Procedure; abbr.: GOBT).

Art. 17 GG determines that a petition has to be filed in writing. Traditionally, "in writing" requires a piece of paper with the petition text on it, signed by the petitioner. Accordingly, 4 (1) of the Rules of Procedure of the Bundestag's petition committee (RoP BT) states the written form requirement and adds that it is also observed if the petitioner uses the online form and provides her name and postal address. However, this data is not published on the petition platform; everyone who wants to contribute to the platform has to register.

The name and permanent address data of a public ePetition's so-called main petitioner ("initiator of a public petition") is published online together with the petition text (Nr. 6 of the additional Directive on public ePetitions, [18]). Signees have to register, but can choose to sign the petition under a pseudonym (created by the system). However, this only provides pseudonymity towards other users of the platform.

At the same time, the Bundestag introduced a discussion forum to allow interested parties to discuss a public petition's content. Participation in the forum discussions is only possible under a self- or system-chosen pseudonym [2]. Petitions including signee lists and contributions to the discussion forum are accessible online throughout three election periods before they are deleted.

It is questionable whether petitions may be filed online in Germany at all. The electronic form could be regarded as constitutionally excluded: According to the jurisdiction of the German constitutional court, it is constitutionally not permissible to conduct parliamentary elections in Germany solely electronically. In a parliamentary democracy the elections of the representatives are the initial and the key element of the chain of democratic legitimacy. Based in this appraisal, the German constitutional court in its grounds mainly refers to the principle of publicity of elections which is derived from Art. 38, in conjunction with Art. 20 (1) and (2) GG. The court considered the principle as affected, since the usage of electronic voting machines did not allow monitoring the actual voting process (all relevant steps from the voter's individual action to the result) without having expert knowledge [19]. However, the electoral principles only concern parliamentary or general elections and are not transferable to other democratic instruments [20]. Therefore, the petitions process is not affected by the judgement of the German constitutional court initially mentioned and can be conducted electronically (including online). But at the same time, since the electoral principles are not applicable, no rights can be derived from e.g. the principle of secrecy (Art. 38 (1) GG). In other words: The German constitution does not grant the right to be anonymous to petitioners.

Since the Bundestag – resp. its petition committee –accepts petitions that are filed via the online form provided at the Bundestag's website, the definition of "in writing" obviously has been adjusted to the modern world. This is not an exception. § 3a of the federal German Administrative Procedure Act stipulates that – if written form is mandatory by law – it may be replaced by electronic form if this is not excluded by (another) legal norm. In context with the eGovernment movement, it is often said that, in general, there are too many written form requirements (e.g. by ISPRAT, [21], p. 4).

A decrease of written form requirements to simplify or facilitate the proceedings should not have a negative impact on the reliability or sincerity of the respective declaration of intent in sensitive areas. Therefore, it needs to be considered carefully which written form requirements may be abdicable. For this, it has to be analyzed individually why written form is required first.

According to the traditional understanding, the written form requirement in Art. 17 GG is necessary because it (a) allows to identify the petitioner, (b) allows to answer the petition (send a notice), and (c) assures the seriousness of the petitioner's request ([22], marginal 61). Sometimes it is also stated that the (d) anonymous exercise of fundamental rights is "a contradiction in terms" ([22], marginal 62).

Here, the written form requirement in Art. 17 GG itself is not to be questioned. But it will be discussed that an online petition platform that employs Privacy-ABCs could fulfill all the requirements set up by the traditional understanding of "in writing" and at the same time protect the petitioner's privacy. A system that applies Privacy-ABCs allows to "identify" the petitioner (criteria (a) from the list above), since the system

guarantees that the one who participates is duly accredited. It is not necessary to know the name of the petitioner if it is assured that she exists and has the right to petition. Insofar, as the nationality or permanent residence of the petitioner is of relevance (e.g. any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State can petition the European Parliament, cf. 215 (1) RoP EP), the petitioner will only have to prove the country to the system and will be allowed to file her petition. There is no need for the recipient to learn about the exact address of the petitioner.

A Privacy-ABC system allows contacting the petitioner (criteria (b)). It is possible to implement some sort of chat functionality. The petition committee could communicate its decision online. Another, and probably the preferable, option could be to implement a system which offers a "sharing documents" functionality. In a Privacy-ABC-based communication system it is possible to implement a personal "Restricted Area" for every user ([23], pp. 19, 33). This allows the petition committee to upload the petition notice (as a document) to the respective petitioner's Restricted Area. Only the petitioner will have access to this area and, consequently, to the document. The system guarantees that only the petitioner can retrieve this document.

Finally, it is not reasonable that an online form can guarantee the seriousness of a petitioner's request less than, say, a post card – which, by the way, would fulfill the "in writing" requirements if signed with name (criteria (c) and (d)). Still this online form exists today and therefore apparently is regarded as compliant with the constitution. Occasionally it is even doubted that a petition to the Bundestag filed online enjoys the protection by the constitution because it does not fulfill the constitutionally prescribed form requirements ([24], p. 59). But if the public authorities open this door, a discrimination of ePetitions is not acceptable.

Due to the fact that the fundamental right to petition is meant to be exercisable as easily as possible and therefore no other procedural requirements need to be fulfilled ([25], marginal 38), it is worth to make it accessible as easy as technically and legally possible. Especially due to the fact that petitions often are regarded as the "ultimate backup" or an "emergency telephone" for the citizens ([3], p. 36), it would be inappropriate to create artificial obstacles. In contrary, all discretion should be used and bureaucratic requirements – such as a necessarily postal communication with the petitioner, once the petition is filed – rethought.

Schleswig-Holstein. In the German federal State of Schleswig-Holstein the idea of anonymous ePetitions was proposed by a Member of Parliament, but has not met with broad support by the responsible committees, yet.

The right to petition the Parliament of Schleswig-Holstein (Landtag) is not explicitly laid down in the constitution of Schleswig-Holstein, but arises from the federal constitution, which – of course – also is applicable at federal state level. The constitution of Schleswig-Holstein (abbr.: LVerf S-H) just states that the State Parliament shall establish a petition committee (Art. 19 (1) LVerf S-H). So the right to petition is not stated, but preconditioned. The procedural rules are similar to those of the Bundestag, in particular they also foresee public ePetitions. Since the minimal conditions arise from the constitution (i.e. the GG), the same approach as on German federal

level (see above) should be applied here. An online platform that allows anonymous (public) ePetitions would be legally permissible.

4 Obstacles to Overcome

Since a democratic system provides instruments of participation, these instruments should be accessible and attractive to as many citizens as possible. Therefore, potential obstacles have to be removed. Based on the assumption that participating online – via an own device, from wherever the user is – is convenient, the next step is to discuss if citizens feel comfortable with raising issues and expressing their opinion towards the public authorities, and if they do not, how the offer can be improved. In the following section, major concerns regarding online petition platforms are addressed in order to show that a Privacy-ABC-based system might foster the democratic participation.

4.1 Fear of Discrimination by Other People or Public Authorities

In principle, a petition can address any subject. However, most petitions will at least indicate the political opinion of the petitioner (and the signees). The sensitivity of personal data can also result indirectly from the context ([26], rec. 56a). This may keep people from participating, since they fear negative consequences, or to be attacked for their opinion. The data protection legislation provides stricter requirements concerning the processing of data about political opinions. It is defined as sensitive data (cf. Art. 8 Dir. 95/46/EC). Against this background, the fact that a petitioner has to identify herself with her full name and permanent address towards the public authorities is unsatisfactory not only from a privacy perspective. Especially, it is incomprehensible why the name and permanent address of the initiator of a public ePetition has to become known even to the Internet public. In fact, it would be sufficient to publish the petition text and use a pseudonym here as well – as for the discussion forum, in the case of the Bundestag. On the European level public ePetitions do not exist. But in general, the European Parliament seems to be aware of the problem and thus allows exceptions from its rule to publish petition texts including the petitioners' names.

Anonymity could prevent a (theoretical) possible "there you go again"-reflex of the petition committees in cases of people who petition repeatedly. In general, anonymous petitions allow the most objective and fair decision by the petition committees, as nothing but the content (and maybe the number of signees) is known to them. In fact, very few petitioners are "heavy users". Most of the users of the Bundestag's online platform do not sign more than two petitions ([3], p. 79]. This may also mean: The fewer "troublemakers", the more likely it becomes that they are known by name.

4.2 Data Security / System Data Protection

There is a difference between "being on a list that, if any, can be consulted at a town hall" – as in case of a traditional referendum, for instance – and "being on a list that is published online". The latter is potentially considerable by the whole online world and – since the information is stored on the public authorities' servers – of course, potential target of cyber criminals (data theft). So, even if one does not fear discrimination by the public entities or other users, such security threats have to be considered. As for parliamentary elections, 57 % of the German citizens would prefer not to vote online for doubts about security in general. 37 % explicitly fear misuse of their data [27]. At the same time, nearly three out of four Germans (74 %) expect the government and business community to actively ensure online security ([28], pp. 9-10). And at least nearly 60 % of Germany's population assumes that responsibility for security and data protection on the Internet primarily rests with companies and/or the government, which they expect to create the necessary conditions ([28], p. 12).

Having said this, it is obvious that such data security problems cannot simply be solved by not publishing the names of petitioners (and signees) online. The less data is stored centrally, the better. Already if information is stored that allows re-identification or linkage to other databases, an attacker could use this information in connection with information stored in service or log files of other data controllers to identify a participant. Since with Privacy-ABCs only the information absolutely necessary is revealed to the service provider, the petition committees', resp. the parliaments', servers would have to deal only with a small amount of data (cf. Section 2.3). The data minimization and data avoidance principle addresses this risk. It demands that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6 (1) (c) Dir. 95/46/EC). If an anonymous or pseudonymous mode of use is possible, the user shall have this opportunity ([26], marginal 1, 4). A Privacy-ABC-based system could fulfill the requirements arising from the data minimization and data avoidance principle.

4.3 Multiple Participation

Another issue – not from a privacy, but general eGovernment perspective – is to prevent users from participating several times. For instance, the RoP BT determine that if a public ePetition is signed by at least 50,000 people, the petitioner (or several petitioners) will be invited to a personal interview by the petition committee, while normally there is no right to be heard. Even if this may not be considered as a big issue concerning ePetitions, it can be of interest for further use cases such as citizens' initiatives and referendums. In these cases even more rights arise from the achievement of a certain quota.

The current ePetition system of the Bundestag, for instance, checks the e-mail address and the IP address of a signee ([3], p. 74). In times of dynamic IP addresses this is clearly not the most reliable method to exclude multiple participations. A Privacy-ABC system, for instance, could be implemented in a way that in case of repeated

participation in the petition, only the last signature would be counted (cf. [29], p. 85; [5], p. 213).

4.4 Contact the Petitioner

As indicated above, the petition committees are legally obliged to send a note to the petitioner in order to communicate its decision. This issue has already been addressed in Section 3.2 when discussing reasons for the written form requirement on German federal level.

4.5 Misuse

Cases of misuse are rare under the current Bundestag system ([3], p. 15]). Considering the fact that at present people could "invent" identities (e.g. by using an assumed name and creating a fake e-mail account), this is in a way remarkable. However, public authorities might fear that anonymity would open up for every conceivable kind of abuse. A public ePetition to the Bundestag is inadmissible, inter alia, if it contains obviously wrong, distorting or offensive expressions. The same holds if the content is obviously impertinent or is based on fundamentally wrong premises. In principle, deletion seems to be sufficient in such cases. But at present, the petition committee could demand criminal prosecution and provide the respective authorities with potentially identifying data, such as the IP address.

However, if a Privacy-ABC-based system including the inspection feature (as described in Section 2.2) was employed, the identification of the user would be regulated. Although it is explicitly not intended at this point to vote for an "all identifiable system through the back door", it might be considerable that it is fairer to let the user know the exact conditions under which her identity will be revealed. This would be the case in a Privacy-ABC system with an implemented inspection feature. At the same time, a Privacy-ABC system would provide a strong authentication. Misuse in terms of illegitimate petitions by illegitimate users could be prevented.

5 Conclusions

It was shown that all guarantees arising from the actual fundamental right to petition can be granted when introducing an anonymous ePetition system which employs Privacy-ABCs. The right to petition is designed as "low barrier" (in terms of "bureaucratic hurdles") democratic instrument and therefore the ideal environment for a completely new and innovative approach. If someone is legitimated to make use of the right to petition, the proof of this legitimization (i.e. being a citizen, living in a specific region etc.) is sufficient. Whether the concern brought up in the petition is legitimate as well is a different matter and does not depend on the person's identity.

The benefit of respecting the citizens' fundamental right to privacy is not just a goal in itself. Even if at the moment most people in Europe live in countries that respect their citizens' rights, unfortunately it cannot be granted that it will stay this way.

In the recent past, the European Community has seen political developments in some Member States which indicate that the guarantees of freedom and expression are not as perfectly natural as one may wish for. They need to be watched and defended. Democracy does not work if no one participates due to fear of consequences. Instruments like the petition are a comparatively easy way to report wrongdoing. They deserve reasonable assistance and support from the democratic forces that can be offered.

References

1. Märker, O., Wehner, J.: E-Participation. In: Zechner, A. (ed.) E-Government Guide Germany, pp. 355-369. Fraunhofer IRB Verlag, Stuttgart (2007)
2. Deutscher Bundestag: Petition zur Veröffentlichung einreichen (2015), https://epetitionen.bundestag.de/epet/peteinreichen/oeffentlich.schritt1.html (Accessed 9 March, 2015)
3. Riehm, U., Böhle, K., Lindner, R.: Elektronische Petitionssysteme: Analysen zur Modernisierung des parlamentarischen Petitionswesens in Deutschland und Europa. Edition sigma, Berlin (2013), http://www.itas.kit.edu/pub/v/2013/riua13a.pdf (Accessed 9 March, 2015)
4. Bieker, F., Hansen, M., Zwingelberg, H.: Towards a privacy-preserving inspection process for authentication solutions with conditional identification. In: Hühnlein, D., Roßnagel, H. (eds.): Proc. Open Identity Summit 2014. Lecture Notes in Informatics, vol. P-237, pp. 85-96. Gesellschaft für Informatik, Bonn (2014), http://subs.emis.de/LNI/Proceedings/Proceedings237/article2.html (Accessed 9 March, 2015)
5. Diaz, C., Kosta, E., Dekeyser, H., Kohlweiss, M., Nigusse, G.: Privacy preserving electronic petitions. Identity in the Information Society, vol. 1, issue 1, pp. 203-219. Springer Netherlands (2008)
6. Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. WP 216. Adopted on 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (Accessed 9 March, 2015)
7. Abendroth, J., Bcheri, S., Krontiris, I., Liagkou, V., Sabouri, A., Schlehahn, E., Veseli, F., Zwingelberg, H.: ABC4Trust D5.2a Amendment Building Blocks of ABC Technology. Deliverable of the ABC4Trust Project (2013), https://abc4trust.eu/download/ABC4Trust-D5.2a_Amendment_Building_Blocks_of_ABC _Technology.pdf (Accessed 9 March, 2015)
8. Bcheri, S., L. Damgård, K., Deibler, D., Goetze, N., G. Knudsen, H., Moneta, M., Pyrgelis, A., Schlehahn, E., B. Stausholm, M, Zwingelberg, H.: ABC4Trust D5.3 Experiences and Feedback of the Pilots. Deliverable of the ABC4Trust Project (2014), https://abc4trust.eu/download/D5.3_ExperiencesAndFeedback_Final.pdf (Accessed 9 March, 2015)
9. EU Network of Independent Experts on Fundamental Rights: Commentary of the Charter of Fundamental Rights of the European Union (2006), http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf (Accessed 9 March, 2015)

10. Article 29 Data Protection Working Party: Opinion 4/2007 on the Concept of Personal Data. WP 136. Adopted on June 20, 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (Accessed 9 March, 2015)
11. Deutscher Bundestag: Nutzungsbedingungen (2015), https://epetitionen.bundestag.de/epet/service.$$$.rubrik.nutzungsbedingungen.html (Accessed 9 March, 2015)
12. VG Berlin, 1. Kammer: Datenschutzrechtliche Anordnung im Fall der Speicherung von Beschäftigtendaten. Urteil vom 13. Januar 2014, 1 K 220.12 (2014), http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/279b/bs/10/page/sammlung.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=JURE140003569&doc.part=L&doc.price=0.0#focuspoint (Accessed 9 March, 2015)
13. Bundesgerichtshof: Urteil vom 1. Juli 2014 – VI ZR 345/13 (2014)
14. Bundesverfassungsgericht: BVerfGE 2, 225 – Beschluß des Ersten Senats vom 22. April 1953 – 1 BvR 162/51 (1953)
15. European Court of Justice: Judgment of the General Court (Sixth Chamber) of 14 September 2011. Ingo-Jens Tegebauer v European Parliament. Right to petition – Petition addressed to the Parliament – Decision to take no action – Action for annulment – Actionable measure – Admissibility – Obligation to state reasons. Case T-308/07 (2011), http://curia.europa.eu/juris/liste.jsf?language=en&num=T-308/07# (Accessed 9 March, 2015)
16. European Court of Justice: Judgment of the General Court (Sixth Chamber) of 27 September 2012. J v European Parliament. Right of petition – Petition addressed to the European Parliament – Decision to take no further action – Action for annulment – Duty to state reasons – Petition not falling within an area of activity of the European Union. Case T-160/10 (2012), http://curia.europa.eu/juris/liste.jsf?language=en&num=T-160/10# (Accessed 9 March, 2015)
17. Uerpmann-Witzack, R.: Artikel 17 GG. In: Münch, I., Kunig, P. (eds.): Grundgesetz-Kommentar Band 1. 6th edition, Verlag C.H. Beck, Munich (2012)
18. Deutscher Bundestag: Richtlinie für die Behandlung von öffentlichen Petitionen (öP) gem. Ziff 7.1 (4) der Verfahrensgrundsätze (Engl.: Directive on the Treatment of Public Petitions according to Nr. 7.1 (4) of the Rules of Procedure), https://www.bundestag.de/blob/190940/c0cbbd627e20fcc1519b03dc61db40f3/richtlinie_oeffentliche_petitionen-data.pdf (Accessed 9 March, 2015)
19. Bundesverfassungsgericht: Urteil des Zweiten Senats vom 3. März 2009 – 2 BvC 3/07, 2 BvC 4/07 (2009), https://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html (Accessed 9 March, 2015)
20. Bundesverfassungsgericht: Beschluss vom 16. Juli 1998 – 2 BvR 1953/95 (1998), http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1998/07/rs19980716_2bvr195395.html (Accessed 9 March, 2015)
21. ISPRAT("Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V."): Stellungnahme zum Referentenentwurf der Bundesregierung eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) (2012),

http://isprat.net/fileadmin/downloads/pdfs/20120618__ISPRAT_Stellungnahme_E-Government-Gesetz.pdf (Accessed 9 March, 2015)
22. Klein, H.H.: Artikel 17 GG. In: Maunz, Th., Dürig, G. (eds.): Kommentar zum Grundgesetz. Loose-leaf booklet. Verlag C.H. Beck, München (2011)
23. Bcheri, S., Björk, E., Deibler, D., Hånell, G., Lerch, J., Moneta, M., Orski, M., Schlehahn, E., Tesfay, W.: ABC4Trust D6.3 Evaluation of the School Pilot. Deliverable of the ABC4Trust Project (2014), https://abc4trust.eu/download/Deliverable%20D6.3.pdf (Accessed 9 March, 2015)
24. Kellner, M.: Die E-Petition zum Bundestag: Ein Danaergeschenk. Neue Justiz, vol. 61, no. 2, pp. 56-59. Nomos, Baden-Baden (2007)
25. Krings, G.: Artikel 17 GG. In: Friauf, K.H., Höfling, W. (eds.): Berliner Kommentar zum Grundgesetz. Loose-leaf booklet, Erich Schmidt Verlag, Cologne (2014)
26. Gola, P., Schomerus, R.: § 3 BDSG. In: Gola, P., Schomerus, R. (eds.): BDSG Bundesdatenschutzgesetz. 11th edition, Verlag C.H. Beck, Munich (2012)
27. DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet: DIVSI Milieu Study on Trust and Security on the Internet – Condensed Version. Hamburg (2012), https://www.divsi.de/publikationen/studien/divsi-decision-maker-study-on-trust-and-security-on-the-internet-condensed-version/ (Accessed 9 March, 2015)
28. DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet: Jeder Zweite möchte online wählen. Press release, August 13, 2013, https://www.divsi.de/jeder-zweite-moechte-online-waehlen/ (Accessed 9 March, 2015)
29. Deibler, D., Engeler, M., Krontiris, I., Liagkou, V., Pyrgelis, A., Schlehahn, E., Stamatiou, Y., Tesfay, W., Zwingelberg, H.: ABC4Trust D7.3 Evaluation of the Student Pilot. Deliverable of the ABC4Trust Project (2014), https://abc4trust.eu/download/Deliverable%20D7.3.pdf (Accessed 9 March, 2015)