A View on Privacy & Trust in IoT

Jörg Daubert[a,b] and Alexander Wiesmaier[a] and Panayotis Kikiras[a]
[a]AGT International, Germany
{jdaubert, awiesmaier, pkikiras}@agtinternational.com
[b]Telecooperation Group, Technische Universität Darmstadt / CASED, Germany

***Abstract*—Internet of Things (IoT) technology is rapidly gaining popularity, not only in industrial and commercial environments, but also in our personal life by means of smart devices at home. Such devices often interconnect with cloud services that promise easy usage and global access. However, managing the balance between trust in the service provider and need for privacy of individuals becomes a major challenge considering automatic exchange of manifold personal information. In this paper, we propose a formal model that establishes a relation between information, privacy, as well as trust, and that automatically maps between these terms while maintaining user control.**

Keywords–Internet of Things, Trust, Privacy

I. Introduction

The Internet of Things (IoT) started to gain new momentum in recent years as the consequence of the rapid growth of internet connected devices. However, security, in particular privacy and trust, remain major challenges as Sicari et al. [1] recently pointed out. IoT applications, such as smart home, which for instance use sensors to recognize room presence to control the light, collect information in the most sensitive and personal domains of our life. In such automated communication the owner takes no active role in communication, but relies on devices and services to act on her behalf. Nevertheless, such personally identifiable information (PII) is not always processed by the owner of the information, but rather by an external service. For instance, smart home equipment suppliers also offer cloud-based services in conjunction with their devices. Moreover, IoT marketplaces have emerged and will continue to emerge [2]. Such marketplace facilitate the trade not only of services but also PII as well. While services in the IoT domain may benefit from analyzing large amounts of PII, the privacy need of PII owners has to be considered as well. Compared with other technological revolutions, IoT has a more profound impact on privacy: first, the exchange of PII in IoT is not as precisely regulated as for instance medical records in healthcare scenarios. Second, IoT penetrates our personal life by means of sensing and acting devices at home and wearables. Prior research tackles the challenges of trust assessment and Privacy Enhancing Technologys (PETs) independently. However, both challenges seem to be interconnected as trusted parties may process private data, whereas our need for privacy seems to increase when an un-trusted party is involved.

This paper analyzes definitions and relations among trust and privacy in Section II, followed by a proposal for a new model to link privacy and trust in a formal way. For that, a user-centric perspective is used, where the owner of PII shares information within an IoT environment while protecting her privacy. Section III discusses multi-dimensional privacy and how it can be mapped to our model. Section IV extends the model to multi-dimensional trust. Section V concludes this paper and provides an outlook onto future work.

II. Privacy, Trust, and Information

This section presents a novel view on the relation between privacy and trust. Manifold definitions of the terms privacy and trust exist. Hence, we first elaboration on the terminology at hand in Section II-A. Second, we propose a model for the relation among these terms in Section II-B

A. Definition of Terminology

Commonly agreed definitions of terms such as trust and privacy do not exist. For instance, Uslaner introduces *trust* as "chicken soup of social life" [3], and thus highlights the mere flavors and mysterious definition of this term. Likewise, multiple definitions for privacy exist. Therefore we summarize definitions and extract a common interpretation from an information centric perspective, i.e., the perspective of a subject that owns the information and wants to share it with a service provider. The focus of information is personally identifiable information (PII) [4] as term summarizing all information that could potentially relate to a person, and is therefore relevant for privacy.

a) Privacy: Maslow identifies a "need for privacy" as a core property of self-actualizing, the tip of his *hierarchy of needs* [5]. Other definitions categorize privacy as requirement in the context of PII, e.g., "personally identifiable information (PII) leaving the control of the person whose PII it is" [6]. More detailed, Lessig defines privacy as the combination of "empowerment to control", "utility to protect", "dignity to establish an equilibrium", and "regulating agent to balance power" [7].

Alongside privacy as property that can be either fulfilled or not, privacy can be measured by a metric. Aimeur et al. [8] measure privacy on a discrete scale from no privacy over soft privacy and hard privacy to full privacy depending on how much PII is cryptographically protected from an attacker. Bohli and Pashalidis [9] model relations between privacy notions, e.g., "strong unlinkability with participant hiding", and map other definitions of anonymity, pseudonymity, and unlikability to their model. The remainder of this paper uses privacy as *a measurement for the need of privacy (protection)*. This definition harmonizes with existing ones as it quantifies the need for privacy (Maslow [5]) while establishing compatibility with the technical definition as a requirement (Poore [6]). Moreover, this definition puts privacy into perspective with the notion PII.

Formally, we assume a metric $\mathcal{P}$ for privacy that can be normalized to the interval $\mathcal{P} \in [0, 1]$, indicating $\mathcal{P} = 0$ for no

privacy and $\mathcal{P} = 1$ for absolute privacy in the corresponding metric. For example, k-anonymity [10] can be normalized to $\mathcal{P}_{k-anon} = k/n$ where n is the full population of records (information) and k the size of indistinguishable records, and thus the anonymous subset.

b) Trust: Uslaner uses the chicken soup of social life metaphor to describe trust [3]. For Bao and Chen trust is a compound of the properties "honesty, cooperativeness, and community interests" [11]. According to Poore, trust follows the definition of privacy and is "the assurance that PII will be only used as agreed and will be protected against unauthorized access" [6]. Leister and Schulz follow the notion of trust as a scalar metric [12].

Following the information centric perspective, we define trust as *a measurement for the need of trust*, similar to privacy. This definition mirrors trust assessment approaches, e.g., recommendation and reputation systems, which calculate the trustworthiness of one subject to match it against the need for trust of another subject.

Formally, we define (analogously to privacy) trust $\mathcal{T}$ as a metric normalized to $[0, 1]$ where $\mathcal{T} = 0$ means no trust at all and $\mathcal{T} = 1$ stands for universal trust. For example, in [13] the authors show that a probabilistic model can extend a *no/partial/yes* model in GnuPG to a continuous $[0, 1]$ trust scale for the authenticity of public keys.

c) Sensitivity: Existing definitions of privacy and trust relate to the term PII, however definitions of PII itself differ as well. European law categorizes information into two classes, information covered by Directive 95/46/EG [14] (PII), and all other information (non-PII). Narayanan et al. further subdivide PII into directly identifying, e.g., a unique citizen ID number, compared to conjunctive identifying, e.g., name, place, and date of birth [15]. Jabeur et al. distinguish minimum, medium, and maximum sensitivity for PII in such a hierarchy [16]. Role-based access control mechanisms establish relations among roles [17] to reflect a multitude subdivisions regarding the sensitivity of the controlled information.

To generalize these concepts, we define sensitivity of information $\mathcal{S}$ as a metric normalized to $[0, 1]$. For example following Directive 95/46/EG, we measure a directly identifying information with $\mathcal{S} = 1$ whereas a conjunctive identifying information is measures as $\mathcal{S} = 1/n$ with n denoting the number of required items of information for unique identification.

B. Relations among privacy and trust notions

With the definitions of privacy, trust, and sensitivity, this section elaborates on the relations among these notions.

We propose the relation given by Equation 1 to connect trust to privacy, privacy to sensitivity, and sensitivity to PII. This relation follows the insight that a higher need for trust is caused by a higher need of privacy. The need for privacy is consequently higher the more sensitive information is. Finally, the sensitivity of information depends the actual information (PII) itself.

$$\mathcal{T} \longleftrightarrow \mathcal{P} \longleftrightarrow \mathcal{S} \longleftrightarrow PII \tag{1}$$

Via this relation, it becomes algorithmically decidable how much trust is required to process given PII. Likewise, it becomes decidable what PII can be provided given a certain level of trust. The next paragraphs discuss how such a mapping can be implemented such that it becomes algorithmically decidable.

a) Sensitivity: The sensitivity $\mathcal{S}$ is a metric for PII and therefore is defined by a function *sensitivty* that takes PII as input domain and provides $\mathcal{S}$ as output domain (Function 2).

$$sensitivity\text{: } PII \longrightarrow \mathcal{S} \tag{2}$$

To illustrate this mapping, we assume 20 elements of PII in partial order according to their sensitivity as an example. Figure 1 depicts sensitivity $\mathcal{S}$ over PII as given by some regulation (circles, red) versus PII owner specified preferences (triangles, blue). Elements $1 \ldots 4$ are hardly suitable to identify a person, elements $5 \ldots 16$ require many to few other items to identify a person, whereas elements $17 \ldots 20$ uniquely identify a person. As elements $5 \ldots 8$ illustrate, the owners' judgement regarding sensitive may deviate from regulation.

The mapping to sensitivity rather than dealing with raw PII has the following advantages: first, a unified representation incorporating all laws, regulations, and policies. Second, the possibility for the owner of the PII to express personal preferences. Third, the function *sensitivity* can be based solely on how sensitive the PII is considered without the need to consider sharing of information and trust in service providers yet. In Figure 1, rules, regulation, and policies are considered as a default, a minimal consensus. The user may override this default with his own utility function for sensitivity.

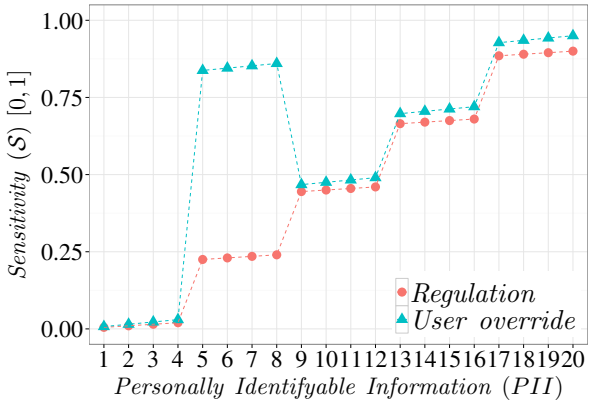

Figure 1. Information sensitivity over PII. The function models the personal view on how sensitive information is.

b) Privacy: The mapping from sensitivity to privacy shows how much privacy is desired given a certain sensitivity of information. As the notion of sensitivity is already established, it is not necessary any more to consider individual elements of PII. Therefore this mapping can be applied to a continuous scale rather than a discrete one. We use Function 3 to formalize this mapping.

$$privacy\text{: } \mathcal{S} \longrightarrow \mathcal{P} \tag{3}$$

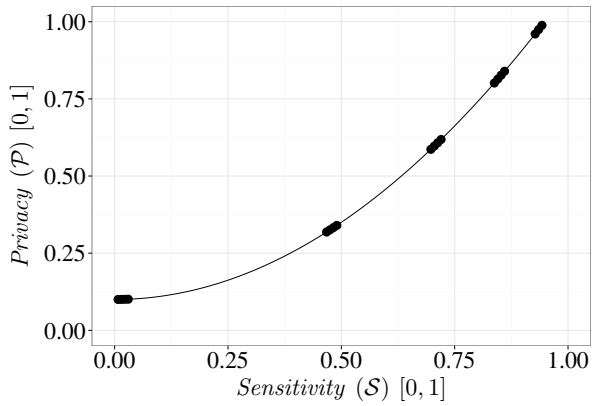

Figure 2. Privacy over sensitivity. The function models the owners' need for privacy. The dots show the application to the 20 example items.

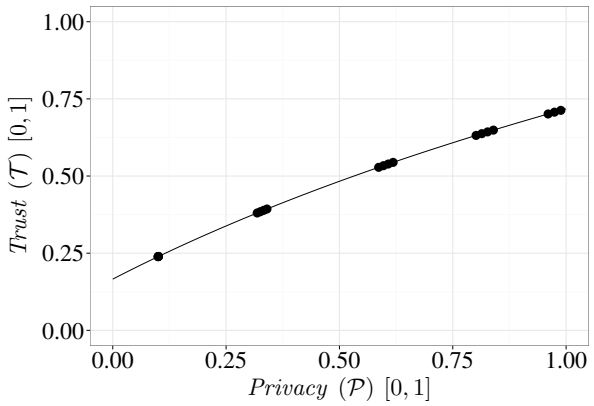

Figure 3. Trust of privacy. The function models the personal need for trust.

Figure 2 illustrates the mapping from sensitivity to privacy using the sample data introduced in the previous paragraph. We use the owner defined Function 4 as an example to model a particular instance of this mapping. Here, the owner always desires a minimum of privacy (constant component $+0.1$) and considers sensitive information exponentially more private (component $\mathcal{S}^2$).

$$\textit{privacy}(\mathcal{S})_{example} \;:=\; \mathcal{S}^2 + 0.1 \tag{4}$$

Our model enables the formalization of privacy without having to consider PII directly, i.e., it provides a layer of abstraction. Furthermore, privacy can be easily customized to fit the needs, e.g., a regulation that applies to multiple PII owners as well as personal preferences of PII owners as in the example.

c) Trust: The notion of privacy so far represents the view of one owner of PII. Trust finally incorporates a second party, the service provider that desires PII. The need of trust $\mathcal{T}$ expresses how much trust the PII owner has to invest in the service provider—or how trustworthy the service provider has to be.

For example, the owner wants to process PII using smart home cloud service providers. Then the owner first uses a computational trust framework such as from Habib et al. [18]. Second, the owner obtains the trust scores of cloud services providers according to own criteria and weight. Third, the owner specifies a $trust_{serviceX}$ function for every cloud service provider X according to scores' uncertainty and personal beliefs. Finally, the model can calculate, compare, and thus automatically decide if the cloud service provider X fulfills the desired level of trust.

Function 5 formalizes the mapping between privacy and trust.

$$\textit{trust: } \mathcal{P} \longrightarrow \mathcal{T} \tag{5}$$

Figure 3 illustrates such a mapping for our example with the mapping Function 6 as an instance of an owner defined function. This function requires the service provider to show significant trustworthiness, even for hardly private data. The function also acknowledges that a trust desire of 100% can be rarely fulfilled and thus a reasonably trustworthy service provider may handle all PII.

$$\textit{trust}(\mathcal{P})_{example} \;:=\; log_3(\mathcal{P} + 1.2) \tag{6}$$

Our model only requires a loose coupling between privacy and trust via an owner customizable function. As a result, the trustworthiness assessment can be obtained from an arbitrary system, while the the calculation of sensitivity and privacy can be performed independently.

d) PII to Privacy: The formal representation of our model can be used to directly calculate privacy desire given PII. By combining Functions 2 and 3, we obtain Function 7, as well as Function 8 for the example.

$$\textit{privacy}' :\; \textit{PII} \;\longrightarrow\; \mathcal{P} \tag{7}$$

$$\textit{privacy}'(\textit{PII})_{example} \;:=\; \textit{sensitivity}(\textit{PII})^2 + 0.1 \tag{8}$$

Figure 4 illustrates this mapping for our example. Such a representation empowers the data owner to explore and understand the influence of PII classification on privacy.

e) Sensitivity to Trust: Similar to the previous paragraph, we also use this model to explore the relation between sensitivity and trust. Functions 9, as well as Function 10 for the example, formalize this relation.

$$\textit{trust}' :\; \mathcal{S} \;\longrightarrow\; \mathcal{T} \tag{9}$$

$$\textit{trust}'(\mathcal{S})_{example} \;:=\; log_3(\mathcal{S}^2 + 1.3) \tag{10}$$

Figure 5 illustrates this mapping for our example. Such a representation empowers the data owner to explore and understand how sensitive information might be to be handled by a service provider given the trustworthyness.

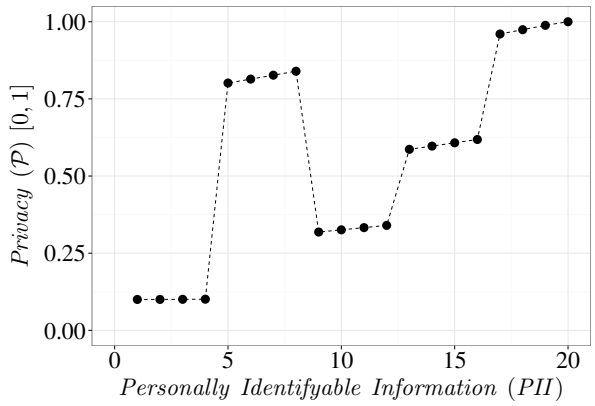

Figure 4. Privacy of PII via implicit sensitivity.

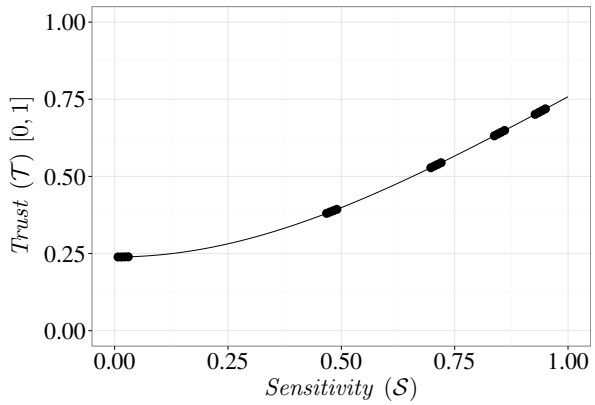

Figure 5. Trust of sensitivity via implicit privacy.

f) Summary: PII to trust: The presented three mappings, from PII to sensitivity, from sensitivity to privacy, and from privacy to trust allow the owner to model personal preferences individually by defining the mapping functions. By combining all three functions, this formalization translates from PII to trust need while remaining customizable and transparent. Function 11 formalized this relation, and Function 12 completes the example.

$$trust'' : PII \longrightarrow \mathcal{T} \quad (11)$$

$$trust''(PII)_{example} := log_3(sensitivity(PII)^2 + 1.3) \quad (12)$$

Figure 6 illustrates this mapping for our example. Such a representation empowers the data owner to explore and understand exactly what PII can be handled by a service provider given a certain trustworthiness.

III. Dimensions of Privacy

In Section II-A, we elaborate on definitions for the term privacy and establish privacy as a scalar metric $\mathcal{P}$ for the mapping in between sensitivity and trust. However, literature suggests that privacy is perceived as a multi-dimensional metric rather than a scalar. Therefore, we discuss our model in the context of multi-dimensional privacy. Based on that

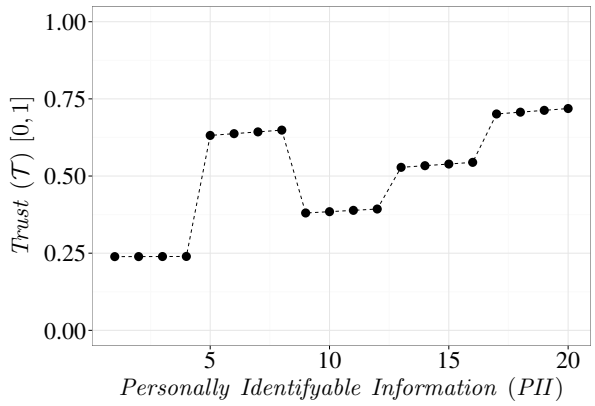

Figure 6. Combined transitional mapping from PII to trust need.

model, we propose a multi-dimensional version of the mapping between trust and and PII, i.e., we introduce the metric $\vec{\mathcal{P}}$ as an extension of $\mathcal{P}$.

Barker et al. categorize privacy of PII alongside the dimensions purpose, visibility, as well as granularity, and propose a 4-dimensional representation of privacy that includes the duration of the permitted usage as well [19]. Domingo-Ferrer establishes a 3-dimensional representation of privacy with respect to the involved entities: the owner who controls the PII, the service provider (called respondent) who leaks information by answering a questions, and the user who leaks information by asking the service provider a question [20].

These definitions express privacy in a context, e.g., where the data is shared, who accesses it, and for which purpose. To complement these definitions, this papers discusses the question "How private is this piece of PII?" from the owners' perspective. Hence we measure sensitivity and privacy along dimensions of the origination of PII rather than their destination.

Privacy can be categorized along several dimensions [21]. The next paragraphs briefly discuss four of these dimensions, namely identity privacy, location privacy, footprint privacy, and query privacy. Other sets of privacy dimensions may be argued and are also applicable to our model.

A. Identity Privacy

Identity privacy refers to the need of privacy for information that can identify a person. Many approaches [22], [23], [10] have been proposed to comply to this need, e.g., by performing pseudonymization or anonymization of such PII. Likewise, approaches to de-anonymize persons from such protected information have been proposed [24], [15].

B. Location Privacy

Location privacy refers to a specific and widely researched form of footprint privacy. Location can reveal manyfold PII, e.g., points of interest [25] and thus even the religion given by the location of a church. Therefore approaches to comply to the need of location privacy such as MIX-zones [26] and sharing of location slices [27] have been proposed.

C. Footprint Privacy

Footprint privacy refers to the privacy need for all PII that gets leaks unintentionally, e.g., preferred language and operating system when browsing the web. Such data is also referred as metadata and micro data. Like identity privacy, approaches to fulfill this need exist [28]. However, the sole fact of *acting* may leave a footprint without the possibility of avoidance.

D. Query Privacy

Query privacy refers to need for privacy regarding the PII contained in a query, e.g., weather forecasts require location and date. Methods for answering queries wile respecting the need for privacy exist [29], however the fact that a query has been made is hardly hideable, e.g., the fact someone is interested in weather.

E. Multidimensional Privacy

We extend the privacy metric $\mathcal{P}$ to $\vec{\mathcal{P}}$ as defined by Equation 13 to reflect the multiple dimensions of privacy, and to allow the owner to specify personal preferences in each dimension independently.

$$privacy: \ \mathcal{S} \longrightarrow \vec{\mathcal{P}} \tag{13}$$

IV. Dimensions of Trust

In Section II-A, we deal with some definitions of trust and establish trust as a scalar metric $\mathcal{T}$ that is later on mapped to privacy, sensitivity and PII. As with privacy, literature suggests that trust is rather a multi-dimensional metric and we introduce the notion of multi-dimensional trust and expand our model by $\vec{\mathcal{T}}$.

Roman et al. split trust into the two dimensions of "trust in the interaction between entities" and "trust in the system from the point of view of the user" [30]. Likewise, Hochleitner et al. distinguish between system trust and interaction trust [31]. Bao and Chen identify three trust properties honesty, cooperativeness, and community interest [11].

As with privacy, we follow a user centric approach and aim for answering the question "How trustworthy is the service provider for this PII?". Hence we measure trust along dimensions of the handling of the PII and compare the trust assessment with the trust need.

The next paragraphs briefly discuss four of these dimensions, namely device trust, processing trust (service provider), connection trust and system trust (overall perspective). Other sets of trust dimensions may be argued and are also applicable to our model.

A. Device Trust

Device trust refers to the need to interact with reliable devices such as sensors and actuators. Common approaches to meet this goal are trusted computing [32] and trusted software [33].

B. Processing Trust

Processing trust expresses the need to deal with correct and meaningful data. This is usually achieved by accurate data gathering combined with suitable data analytics. The results may be further improved by data fusion.

C. Connection Trust

Connection trust stands for the requirement to exchange the right data with right service providers and only with them. This is achieved by ensuring canonical security goals such as confidentiality, authenticity, and non-repudiation.

D. System Trust

System trust refers to the desire to leverage a dependable overall system. This kind of trust is commonly achieved by providing transparency to all involved subjects regarding workflows, processes, underlying technology an so on, e.g., by passing respective certifications.

E. Multidimensional Trust

We extend the trust metric $\mathcal{T}$ to $\vec{\mathcal{T}}$ as defined by Equation 14 to reflect the multiple dimensions of trust. Note that we make use of the previously introduced multidimensional privacy metric $\vec{\mathcal{P}}$. Altogether we then come to the multi-dimensional model as expressed by Equation 15.

$$trust: \ \vec{\mathcal{P}} \longrightarrow \vec{\mathcal{T}} \tag{14}$$

$$\vec{\mathcal{T}} \longleftrightarrow \vec{\mathcal{P}} \longleftrightarrow \mathcal{S} \longleftrightarrow PII \tag{15}$$

Multidimensional trust can be visualized to user for instance via radar charts. Even variations that incorporate uncertainty in case trust cannot be assessed absolutely exist [34] and seem to be easy to assess by users.

V. Conclusion

This paper presents a novel view on the relations between PII, sensitivity of information, privacy, and trust. Furthermore, these relations can be expressed in a formal way, but yet abstracts complexity by decoupling the need for trust from PII. We also showed that this formal mapping can be expressed in a multi-dimensional space to express the need for privacy fine-grained, e.g., according to identity, location, query, and footprint.

We expect that this model will easy new application scenarios in the IoT, Machine 2 Machine (M2M), as well as the Big Data domain where sharing of PII is rapidly evolving towards an automated process. Future work will address the challenge of leveling gaps between the need for trust provided by the data owner and the trustworthiness of a service provider. In particular, we will model the type of service provider as another dimension to express multiple service providers and personal preferences towards them in one model. This work can be included into automatic policy negotiation frameworks in conjunction with PETs.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, 2015, pp. 146–164.

[2] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," IEEE Access, vol. 2, 2014, pp. 1660–1679. [Online]. Available: http://dx.doi.org/10.1109/ACCESS.2015.2389854

[3] E. M. Uslaner, The moral foundations of trust. Cambridge University Press, 2002.

[4] A. Narayanan and V. Shmatikov, "Myths and fallacies of "personally identifiable information"," Commun. ACM, vol. 53, no. 6, 2010, pp. 24–26.

[5] A. H. Maslow, "A theory of human motivation." Psychological review, vol. 50, no. 4, 1943, p. 370.

[6] R. S. Poore, "Anonymity, privacy, and trust," Information Systems Security, vol. 8, no. 3, 1999, pp. 16–20.

[7] L. Lessig, Code and other laws of cyberspace. Basic books, 1999.

[8] E. Aïmeur, S. Gambs, and A. Ho, "Towards a privacy-enhanced social networking site," in ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland. IEEE Computer Society, 2010, pp. 172–179.

[9] J. Bohli and A. Pashalidis, "Relations among privacy notions," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, 2011, p. 4.

[10] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, 2002, pp. 557–570.

[11] F. Bao and I. Chen, "Trust management for the internet of things and its application to service composition," in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, USA, June 25-28, 2012. IEEE Computer Society, 2012, pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/WoWMoM.2012.6263792

[12] W. Leister and T. Schulz, "Ideas for a trust indicator in the internet of things," in SMART 2012, The First International Conference on Smart Systems, Devices and Technologies, 2012, pp. 31–34.

[13] J. Jonczy, M. Wüthrich, and R. Haenni, "A probabilistic trust model for gnupg," in Proceedings of the 23rd Chaos Communication Congress, 23C3, 2006, pp. 61–66.

[14] European Parliament and Council of the European Union, "On the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal, vol. L, no. 281, 1995, pp. 0031–0050.

[15] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in 2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA. IEEE Computer Society, 2008, pp. 111–125. [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=4531131

[16] N. Jabeur, S. Zeadally, and S. Maydebura, "Improving trust and privacy models in social networks," in NTMS, A. Levi, M. Badra, M. Cesana, M. Ghassemian, Ö. Gürbüz, N. Jabeur, M. Klonowski, A. Maña, S. Sargento, and S. Zeadally, Eds. IEEE, 2012, pp. 1–5.

[17] M. Nyanchama and S. L. Osborn, "The role graph model," in ACM Workshop on Role-Based Access Control, 1995.

[18] S. M. Habib, V. Varadharajan, and M. Mühlhäuser, "A framework for evaluating trust of service providers in cloud marketplaces," in Proceedings of the 28th Annual ACM Symposium on Applied Computing, SAC '13, Coimbra, Portugal, March 18-22, 2013, S. Y. Shin and J. C. Maldonado, Eds. ACM, 2013, pp. 1963–1965.

[19] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams, "A data privacy taxonomy," in BNCOD, ser. Lecture Notes in Computer Science, A. P. Sexton, Ed., vol. 5588. Springer, 2009, pp. 42–54.

[20] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," in Secure Data Management, 4th VLDB Workshop, SDM 2007, Vienna, Austria, September 23-24, 2007, Proceedings, ser. Lecture Notes in Computer Science, W. Jonker and M. Petkovic, Eds., vol. 4721. Springer, 2007, pp. 193–202.

[21] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," IEEE Communications Magazine, vol. 51, no. 6, 2013. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2013.6525606

[22] J. Camenisch and E. V. Herreweghen, "Design and implementation of the *idemix* anonymous credential system," in Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002, V. Atluri, Ed. ACM, 2002, pp. 21–30. [Online]. Available: http://dl.acm.org/citation.cfm?id=586110

[23] D. Chaum, "Blind signatures for untraceable payments," in Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982., D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Plenum Press, New York, 1982, pp. 199–203.

[24] A. Narayanan and V. Shmatikov, "How to break anonymity of the netflix prize dataset," CoRR, vol. abs/cs/0610105, 2006. [Online]. Available: http://arxiv.org/abs/cs/0610105

[25] J. Freudiger, R. Shokri, and J. Hubaux, "Evaluating the privacy risk of location-based services," in Financial Cryptography and Data Security - 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 - March 4, 2011, Revised Selected Papers, ser. Lecture Notes in Computer Science, G. Danezis, Ed., vol. 7035. Springer, 2011, pp. 31–46.

[26] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in 2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14-17 March 2004, Orlando, FL, USA. IEEE Computer Society, 2004, pp. 127–131.

[27] Z. Riaz, F. Dürr, and K. Rothermel, "Optimized location update protocols for secure and efficient position sharing," in 2015 Conference on Networked Systems, NetSys 2015, Cottbus, Germany, March 9-12, 2015. IEEE, 2015, p. in print.

[28] R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The second-generation onion router," in Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA, M. Blaze, Ed. USENIX, 2004, pp. 303–320.

[29] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer, 2004, pp. 506–522.

[30] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, 2013, pp. 2266–2279.

[31] C. Hochleitner, C. Graf, D. Unger, and M. Tscheligi, "Making devices trustworthy: Security and trust feedback in the internet of things," in Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 2012.

[32] A. Iliev and S. Smith, "Protecting client privacy with trusted computing at the server," Security Privacy, IEEE, vol. 3, no. 2, March 2005, pp. 20–28.

[33] D. Kirovski, M. Drinić, and M. Potkonjak, "Enabling trusted software integrity," in ACM SIGPLAN Notices, vol. 37, no. 10. ACM, 2002, pp. 108–120.

[34] F. Volk, S. Hauke, D. Dieth, and M. Mühlhäuser, "Communicating and visualising multicriterial trustworthiness under uncertainty," in 2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, Canada, July 23-24, 2014, A. Miri, U. Hengartner, N. Huang, A. Jøsang, and J. García-Alfaro, Eds. IEEE, 2014, pp. 391–397. [Online]. Available: http://dx.doi.org/10.1109/PST.2014.6890965