ICDS 2025

The Nineteenth International Conference on Digital Society

ISBN: 978-1-68558-267-8

May 18 - 22, 2025

Nice, France

ICDS 2025 Editors

Lasse Berntzen, University of South-Eastern Norway, Norway

ICDS 2025

Forward

The Nineteenth International Conference on Digital Society (ICDS 2025), held between May 18th, 2025, and May 22nd, 2025, in Nice, France, continued a series of international events covering a large spectrum of topics related to advanced networking, applications, and system technologies in a digital society. Nowadays, most economic activities and business models are driven by the unprecedented evolution of theories and technologies. The reflection of these achievements into our society is present everywhere, and it is only question of user education and business models optimization towards a digital society.

Progress in cognitive science, knowledge acquisition, representation, and processing helped to deal with imprecise, uncertain, or incomplete information. Management of geographical and temporal information becomes a challenge, in terms of volume, speed, semantic, decision, and delivery. Information technologies allow optimization in searching and interpreting data, yet special constraints imposed by the digital society require on-demand, ethics, and legal aspects, as well as user privacy and safety.

The variety of the systems and applications and the heterogeneous nature of information and knowledge representation require special technologies to capture, manage, preserve, interpret, and deliver the content and documents related to a particular target.

We take here the opportunity to warmly thank all the members of the ICDS 2025 technical program committee, as well as all the reviewers. The creation of such a high-quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to ICDS 2025. We truly believe that, thanks to all these efforts, the final conference program consisted of top-quality contributions. We also thank the members of the ICDS 2025 organizing committee for their help in handling the logistics of this event.

We hope that ICDS 2025 was a successful international forum for the exchange of ideas and results between academia and industry for the promotion of progress in a digital society.

ICDS 2025 Chairs

ICDS 2025 Steering Committee
Lasse Berntzen, University of South-Eastern Norway, Norway
Claus-Peter Rückemann, Universität Münster / DIMF / Leibniz Universität Hannover, Germany
Theo Lynn, Irish Institute of Digital Business, Dublin City University, Ireland
Olga Levina, Technische Hochschule Brandenburg, Germany
Claudia Heß, IU Internationale Hochschule, Germany

ICDS 2025 Publicity Chairs
José Miguel Jiménez, Universitat Politècnica de València, Spain
Francisco Javier Díaz Blasco, Universitat Politècnica de València, Spain
Ali Ahmad, Universitat Politècnica de València, Spain

Sandra Viciano Tudela, Universitat Politècnica de València, Spain
Laura Garcia, Universidad Politécnica de Cartagena, Spain

ICDS 2025
Committee

ICDS 2025 Steering Committee

Lasse Berntzen, University of South-Eastern Norway, Norway
Claus-Peter Rückemann, Universität Münster / DIMF / Leibniz Universität Hannover, Germany
Theo Lynn, Irish Institute of Digital Business, Dublin City University, Ireland
Olga Levina, Technische Hochschule Brandenburg, Germany
Claudia Heß, IU Internationale Hochschule, Germany

ICDS 2025 Publicity Chairs

José Miguel Jiménez, Universitat Politècnica de València, Spain
Francisco Javier Díaz Blasco, Universitat Politècnica de València, Spain
Ali Ahmad, Universitat Politècnica de València, Spain
Sandra Viciano Tudela, Universitat Politècnica de València, Spain
Laura Garcia, Universidad Politécnica de Cartagena, Spain

ICDS 2025 Technical Program Committee

Chiniah Aatish, University of Mauritius, Mauritius
Iván Abellán, University of Luxembourg, Luxembourg
Mohamad Ibrahim Al Ladan, Rafik Hariri University, Lebanon
Laura Alcaide Muñoz, University of Granada, Spain
Ludivine Allienne, Université Picardie Jules Verne - laboratoire CURAPP-ESS, France
Subia Ansari, Purdue University, West Lafayette, USA
Kambiz Badie, ICT Research Institute, Iran
Alessandra Bagnato, Softeam, France
Sanmitra Banerjee, NVIDIA, Santa Clara, USA
Ilija Basicevic, University of Novi Sad, Serbia
Najib Belkhayat, Cadi Ayyad University of Marrakech, Morocco
Lasse Berntzen, University of South-Eastern Norway, Norway
Aljosa Jerman Blazic, SETCCE Ltd. / IT association at Chamber of commerce, Slovenia
Mahmoud Brahimi, University of Msila, Algeria
Justin F. Brunelle, The MITRE Corporation, USA
Erik Buchmann, Universität Leipzig / ScaDS.AI, Germany
Marcos F. Caetano, University of Brasília, Brazil
Maria Chiara Caschera, CNR-IRPPS, Italy
Bidisha Chaudhuri, University of Amsterdam, The Netherlands
Sunil Choenni, Dutch Ministry of Justice and Security / Rotterdam University of Applied Sciences, Netherlands
Yul Chu, University of Texas Rio Grande Valley (UTRGV), USA
Andrei V. Chugunov, ITMO University, St. Petersburg, Russia
Soon Ae Chun, City University of New York, USA
María E. Cortés-Cediel, Universidad Complutense de Madrid, Spain

Qiang Zhu, University of Michigan - Dearborn, USA
Ewa Ziemba, University of Economics in Katowice, Poland

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Investment, Innovation, and Compulsory Spending: A Model of Public-Private Partnerships in Smart City Initiatives

Richard Schilling
Aesir Machina Corporation
Seattle, Washington, USA
email: richard@aesirmachina.com

***Abstract*—This paper examines how public-private partnerships in smart city development may impose compulsory spending through intellectual property costs, impacting local fiscal autonomy and increasing taxpayer burdens. While existing research often highlights the benefits of smart city projects, the assignment of intellectual property rights, particularly patents, remains under-explored. This paper investigates how public-private partnerships in one city can result in assignment of intellectual property rights, and how that in turn can establish mechanisms for compulsory spending in many other cities. Furthermore, this article suggests that such compulsory spending can impact local fiscal autonomy and increase taxpayer burdens. Scenarios where the same investor groups finance multiple projects across different jurisdictions are analyzed, raising concerns about monopolistic control over essential technologies through strategic patent portfolios. This paper concludes that the financial implications for local taxpayers, who ultimately bear the burden and risk of these projects, are frequently overlooked. A framework is proposed to help stakeholders identify such scenarios.**

Keywords-smart cities; governance; United Nations (UN); World Economic Foru (WEF).

I. INTRODUCTION

It is a city's legal obligation to a Public-Private Partnership (PPP) which create the connective tissue between compulsive taxation and the intellectual property owned by the city's contractors. The contractor's control on intellectual property, which is spelled out in the partnership agreements, is structured for the explicit purpose of allowing the contractor to recoup its investment in the partnership [1]. The contractor retains control of intellectual property rights the city relies on and takes control of any new intellectual property. The intellectual property rights on the technology, transferred to the contractor, are what allows the contractor to generate revenue streams far beyond the boundaries of the city where the partnership was created. The revenue streams will be in the form of product sales, contracted services, and technology licensing fees that are paid for by anyone and any city that purchases products based on the contractor's technology. In this way, smart city products and services combined with intellectual property rights give the contractor the ability to not only control who may provide them but also secure a revenue stream from any country that recognizes the contractor's patents. The global scope of the resulting revenue streams allows the contractor to harvest returns that far exceed their costs of developing the technology in the original smart city project. What was once a single's city investment into a novel technology, thus becomes compulsory spending from other cities that rely on it. Ergo, since these cities' resources come from taxes, and tax payments are never voluntary, compulsory spending by these cities to purchase smart city technology can be said to result in taxation.

Sifting through the available information to detect which smart city projects result in compulsory spending can be aided by an analytical framework. However, the vast amount of data available for each project requires a person to choose a framework that can help them put a lens on a smart city project with that purpose in mind. Answering some key questions can help, such as *What framework can help simplify all the available information? What models can be used within the framework? Can the framework be used to determine the value propositions for all stakeholders? And more fundamentally, does the framework rely on a proportional metric of "value" that can be derived for each stakeholder?*

The research project to find analytical frameworks which could answer such questions for smart city projects resulted in the present paper. The research revealed two distinct challenges. First, the definition of "value proposition" is subjective (e.g. financial gain, policy influence, etc.). One person's financial gain on a smarty city project could become another person's financial liability, for example. Second, determining whether the value proposition exists requires the stakeholder to apply an analytical framework to the rich tapestry of information and institutional knowledge attached to the project, which is woven into artifacts such as contracts, documents, policies, databases, lawsuits, and technological innovations. Consequently, defining a proportional metric of "value" that can be derived objectively for all stakeholders is at once challenging and very useful.

We present a framework capable of addressing all three challenges. The framework is based on a proportional metric of value commensurate with each stakeholder's obligations and consequences, not financial picture. Stakeholders are assigned a higher weight of value when they have an obligation to support the smart city project, and a null value when their support of the project is inconsequential. This obligations-based metric simplifies the analysis framework and modeling considerably.

The framework presented is intended to create opportunities to reframe the debate about smart-city projects around an objective analysis, with the taxpayer's interests as stakeholder being a key focus.

This paper is structured as follows. After describing the research method in Section II, the information found about public-private partnerships which is relevant to the framework and model presented in this paper is discussed in Section III. Section IV details the nexus between compulsory taxation and intellectual properties. Section V describes a simplified version of an analysis framework that is typically used to deconstruct and understand smart city projects, and that framework is updated in Section VI.

II. RESEARCH METHOD

Research for this paper was done using a manual review of multiple databases that could provide authoritative sources. A focused literature review was performed, and priority was given to papers and documents that addressed multiple aspects of smart city projects: public-private partnerships, intellectual property, governance, public policy, and technology.

The number papers and relevant documents found were maximized by searching in multiple publication databases that cover the legal, technical, legislative and public policy areas. In general, the databases that provided results for a specific city, in this case Seattle, Washington, USA, contained papers that spanned the broadest set of disciplines. For example, searching for smart city papers in databases maintained by Seattle based organizations yielded papers and documents related to smart city public-private partnerships in academic, legal, technical, public policy, and Seattle specific projects. The same search in databases with a more global reach yielded search results that were relevant to more general technical aspects of smart cities.

Consequently, focusing on Seattle use cases and examples make it possible to tease out the parameters that can be used as the basis of a single analytical framework. The Seattle case is rife with examples that illustrate the challenges of establishing a framework of analysis that provides an objective observer with the means to understand when a smart city project impacts the taxpayer burden in other cities.

The research also revealed that prioritizing papers associated with a specific city, in this case Seattle, yielded very detailed papers addressing legal compliance for smart city projects. For example, the Washington State constitution prohibits the donation of public money to private companies. The legitimacy of a Seattle smart city public-private partnership could be questioned if the financial benefit realized by the city was minuscule compared to the worldwide revenue from the intellectual property tied to the project [2].

All abstracts of ICDS conference papers from 2011 - 2024 were reviewed manually. The body of papers were narrowed down based on abstract content, and a subset of those papers were read in full. The papers that most directly related to the present research topic were selected.

The most productive search terms used included “public-private partnerships”, “ppp”, “smart city public-private partnerships”, “smart city patents”. These same terms were used to find publications at the following places:

- Seattle University Law Review [3].
- The City of Seattle [4].
- King County, Washington. [5].
- The American Journal of Comparative Law [6].
- Elsevier [7].
- Taylor and Francis Online [8].
- World Economic Forum [9].
- US Census Bureau Official Website [10].

In addition, some general google searches were performed using the query “smart city PPP” to find relevant industry information such as Jacobsen’s presentation entitled “Leveraging PPPs for smart city infrastructure” [11].

III. PUBLIC-PRIVATE PARTNERSHIPS IN THE SMART CITY CONTEXT

Public-private partnerships for smart city projects are structured in the same way as other municipal public-private partnerships. A first distinguishing feature about smart city projects, however, is that the city’s choice to form a public-private partnership can be a sign that the project is a “smart city project.” A second distinguishing feature is that the city relies heavily on tech companies to provide products and services [12]. To understand how this might be the case, it is useful to deconstruct that kind of partnership and discuss how it relates to smart city technologies.

Figure 1 shows some common components of a smart city public-private partnership and their relationship to each other.

A. Connecting Stakeholders

In the United States the term public-private partnership denotes government contracts in which the private contractor takes on more responsibility than has been customary [14]. However, a public-private partnership can refer to any type of arrangement that allows the city to shift financing, maintenance and operating costs for public infrastructure to private contractors. The contractors do not bear 100% of the costs of the partnership but share them with the city. Cities have a wide menu of public-private partnership structures to choose from — ranging from contracts for specific services to long-term joint ventures — depending on the city’s role. [11]. While the city’s commitments to the partnership are funded by taxation, the private contractors are allowed to recoup their investment and ongoing costs by charging the public to use of the infrastructure, such as road tolls or usage fees [15]. In the context of smart city infrastructure, the city relies on tech companies to equip the city, and the charges are built into products and services that incorporate intellectual property owned by the contractor [12].

Regardless of the partnership type, however, contractors rely on patents to recoup costs and generate revenue. In addition to providing new revenue streams, patents can be used as a defensive measure - to prevent anyone from interfering with their work on the partnership. They can also generate returns that fund new research programs unrelated to their immediate partnership, which suggests that smart city projects are lucrative enough to regard them as a strategic

growth opportunity, as opposed to just providing a public service [1].

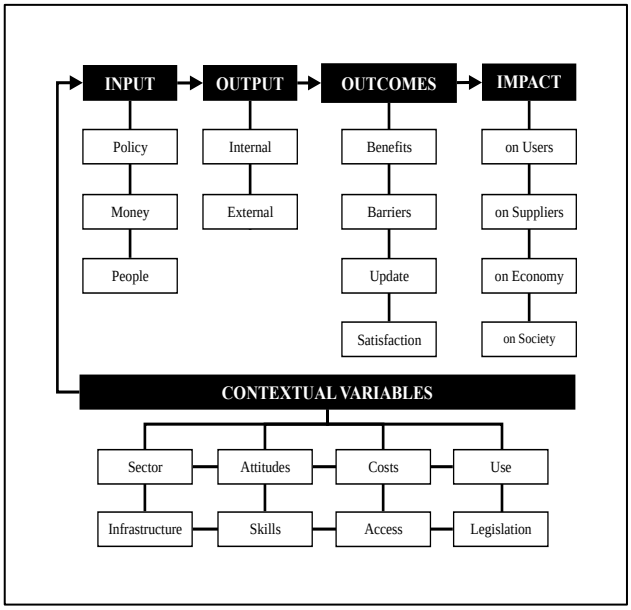

Figure 1. Components of a smart city public-private partnership [13].

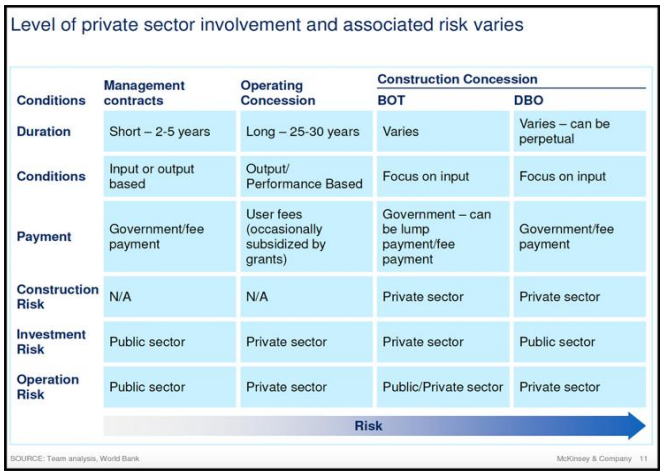

Figure 2. The type of partnership affects how much and type of risk the government entity assumes [11].

Furthermore, the contractor's control on intellectual property, which is spelled out in the partnership agreements, is structured for the *explicit purpose* of allowing the contractor to recoup its investment in the partnership. In such an arrangement the contractor retains control of intellectual property rights the city relies on and takes control of any new intellectual property. The rights assignment aspect of the project emphasizes the important role intellectual property rights have in smart city projects. These rights are often bundled into larger intellectual property portfolios, which can include things like trademark and copyright [15]. A survey of patents related to smart cities indicates that the larger corporations seem to be accumulating patent portfolios related to smart city technology. A portion of the patent counts is presented below in Table I [16].

TABLE I. TOP PATENT FILING COMPANIES IN 2023 [16].

Company	Patent Count
Samsung Electronics	4,035
LG	1,093
Huawei	977
Cisco	966
Intel	446
Vietnam	259
IBM	207
Strong Force IOT	185
Qualcomm	183
AT&T	133

B. *Risk Management*

Contractors, as all city vendors, who participate in smart city projects contend with the same risks that affect any other municipal project [12]. The risks originate from many sources. Some examples include policy goals, local political contexts, availability of federal funding, regulations affecting vendors, and debates over intellectual property. Figure 2 depicts the risks associated with various types of public-private partnerships.

Another risk discussed in literature is corruption. Public-private partnerships are susceptible to corruption risk as well, although it is challenging to document. Some attempts to measure government corruption have been attempted, however they do not address policy issues that lead to it. The design of the contracts involved, the duration of the contracts, and the composition of the actors can make public-private partnerships vulnerable to corruption [17][18].

Given the risks mentioned, clearly the local municipal context has a significant impact on how well smart city partnerships can be managed, especially with respect to the contracts used to set up the project.

C. *Global Agendas*

Companies claim that their research combined with strong patent protections empower them to use smart city projects as technological proving grounds that solve problems facing urban centers such as first/last mile, logistics, traffic congestion, and delivery of e-Government services [19]. However, not all companies are developing new products and technologies. In some instances, venture capital firms are using smart city projects to refresh patent portfolios [16][20][21]. And for some organizations like the World Economic Forum (WEF), the concept of "smart city governance" is marketed as a justification for agendas like the WEF C40, UN 2030 [22]. While a city may only allow the WEF to sponsor a single smart city project, the city agrees to

support the WEF's broader policy goals, some of which are depicted in Table II. The WEF, has stated that its Smart Cities Alliance program is a vector for it to influence governance policy at the local level:

> "Representing more than 200,000 cities and local governments, companies, start-ups, research institutions and non-profit organizations, the Alliance is leading numerous initiatives in more than 36 pioneer cities around the world focusing on smart city governance…" [22]

Clearly for the WEF, establishing a robust influence on local smart city related policies is a multi-fronted effort. In some cases, the WEF seeks to influence local policy through a targeted campaign such as the Global Cities Alliance, as shown in the above quotation. And in other cases, it seeks to inject policy that affects smart city technology through larger programs such as the C40 Cities Initiative. Regardless of what vector is chosen, the result is intended to affect the purchase and use of smart technologies. In 2006 Seattle signed onto the WEF's C40's initiative [22].

While The World Economic forum seeks to leverage smart city projects to support its agenda, the effort draws into sharper contrast the differences between organizations outside the city, and the taxpayers, who fund the city with compulsory tax revenue.

D. Obligation Based Value Propositions

Taxpayers have a unique relationship with the other stakeholders of a smart city public-private partnership, in that they are the only group required to participate through compulsory taxation. The city's participation and the private contractor's participation are voluntary and can even be ended whenever the agreements that underpin a smart city project allow. For example, the individual taxpayer cannot calculate the proportion of their taxes that would be used in a public-private partnership and withhold that from their property tax payments for any reason. Doing so would put the local government in a position of seizing the taxpayer's property such as their home and shutting down their businesses [24].

The relationship taxpayers have with their city illuminates a striking aspect of value propositions in the context of the smart city - the net financial benefit of a smart city project is a moot point for some stakeholders. In Seattle's case there are three concrete examples that illustrate this. Seattle contributed $400,000 to a new AI Incubator which works out to a one-time charge of about $0.53 (fifty-three cents) per taxpayer or less. In another instance, residents pay for local programs based on the value of their homes, which is described in Section IV below. In addition, legal analysis on public-private partnerships in Washington State, where Seattle is located, purposely exclude financial analysis of the various stakeholders [2]. Framing the concept of value proposition based on rote financial calculations, therefore, unnecessarily discard those stakeholders from analysis for whom the smart city project is most consequential.

While an analysis of value propositions based on realized benefits is challenging, assigning a value metric based on their *obligations and consequences* is more straightforward for all cases. Each stakeholder's obligations and consequences are generally spelled out in clear terms in contracts and agreements that communicate the smart city partnership. Table 5 in Section 6, below, illustrates how this concept might be applied.

TABLE II. WEF TARGETS AFFECT THE USE OF TECHNOLOGY AMONG OTHER PRODUCTS [23]

Consumption category	Consumption interventions	Emission reductions per consumption category between 2017 and 2030	Emission reductions per consumption category between 2017 and 2050
	• Reduce the number of new clothing items bought every year • Reduce supply chain waste	39% (Reducing the number of new clothing items alone accounts for 37%)	66% (Reducing the number of new clothing items alone accounts for 64%)
	• Dietary change: eat in line with health recommendations and lower meat and dairy consumption • Reduce household waste • Reduce supply chain waste	36% (Dietary change alone accounts for 27%)	60% (Dietary change alone accounts for 45%)
	• Reduce number of flights • Increase adoption of sustainable aviation fuel	26% (Reducing number of flights alone accounts for 18%)	55% (Reducing number of flights alone accounts for 31%)
	• Improve materials efficiency • Enhance building utilisation • Switch to lower carbon materials • Adopt low-carbon cement • Reuse building components	26% (Improving materials efficiency and enhance building utilisation together account for 18%)	44% (Improving materials efficiency and enhance building utilisation together account for 29%)
	• Reduce car ownership • Increase car lifespans • Increase material efficiency	28% (Reducing car ownership alone accounts for 24%)	39% (Reducing car ownership alone accounts for 31%)
	• Optimise lifetimes of IT equipment	18%	33%

IV. PUBLIC-PRIVATE PARTNERSHIPS CONNECT TAXATION TO INTELLECTUAL PROPERTY PORTFOLIOS

One of the recurring narratives of smart city projects is the notion of the value proposition realized by the taxpayer. Smart city literature available from Seattle reveals that value is often described in overgeneralized terms such as "increasing equity", and this appears to be the case for many of the more politically liberal cities within the United States [26]. A more concrete notion of monetary value, however, can be defined based on hard taxpayer payments if data about those payments are publicly available.

Research by the Tax Foundation provides data that establishes a reasonable data set that can be used for this purpose [27]. A subset of their data is reproduced here:

TABLE III. EFFECTIVE LOCAL TAXES PAID BY RESIDENTS OF CERTAIN CITIES, IN ADDITION TO FEDERAL INCOME TAXES [27].

State	Local Effective Tax Rate
New York	15.90%
California	13.50%
Washington	10.70%

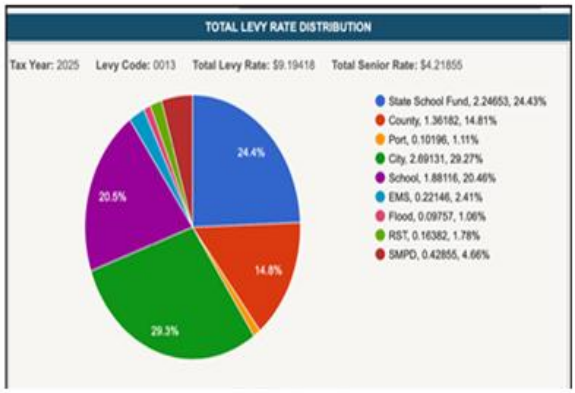

Figure 3. Allocation of homeowner taxes by government program [25].

In addition to effective local tax rates, which can help estimate the average expected tax burden of a city's population, a random selection of property taxes can provide more concrete data. A home in Seattle is presented as an example. Table III shows that the homeowner pays about $66,000/year in property taxes [25]. The use of this revenue paid by the homeowner of this Seattle home is also broken down by program. There are nine different government run programs supported by these taxes (Figure 3), and each program has the authority to create a smart city public-private partnership.

While lump sum property taxes such as these illustrate the overall investment residents currently make into their communities, incorporating them into an analysis framework for smart city projects can lead to misleading results. The literature revealed this can happen for a couple of notable reasons. First, the range of investment attributed to any single taxpayer varies widely. For example, Seattle contributed $400,000 to a new AI Incubator which works out to a one-time charge of about 53 cents per taxpayer. Second, in the legal context the use of monetary values is a moot point. For example, judges in Washington State, where Seattle is located, routinely exclude specific financial information when considering the constitutional aspects of a smart city project [2].

Deconstructing the types of taxes residents pay to fund a city is critical to understanding how public-private partnerships bridge the gap between taxation and intellectual property portfolios. The city itself, at least in the case of the United States, is formed by the residents who live in the area, and the resources a city can make available for smart city projects come ultimately from taxation, either past taxation or future. The power of a city to enter public-private partnerships is created under the authority of the city's charter, which the citizens of the city define during the formation of the city. While the city itself may be the initiator of a public-private partnership, it relies on various types of technologies that will be utilized or created as part of the project. The technologies, in turn, are covered by exclusive rights typically under the control of one of the contractors in the private sector. While the private individuals and companies have a right to profit from the intellectual properties they control, the public has an interest in maintaining basic city infrastructure and services, as well as improving the quality of life [28]. The public-private partnership serves to bridge the gap between private interests and public good within the smart city context.

Because of the tight association between It is helpful to regard the city as a "taxpayer funded startup" for smart city projects, and this is particularly evident when the city invests in actual new business incubators [21].

TABLE IV. AN EXAMPLE OF PROPERTY TAXES PAID BY A SINGLE HOMEOWNER IN SEATTLE, WASHINGTON, USA [25].

Tax Information	2025	2024	2023	2022
Levy code	0013	0013	0013	0013
Status	Taxable	Taxable	Taxable	Taxable
Omit year	0000	0000	0000	0000
Land value	$2,938,000	$2,739,000	$2,739,000	$2,218,000
Improvement value	$4,181,000	$4,108,000	$4,929,000	$3,702,000
Charges				
Tax	$65,453.37	$61,983.90	$62,255.72	$52,270.05
Surface Water	$1,498.72	$1,372.46	$1,290.38	$1,219.00
Noxious Weed	$6.30	$6.30	$6.30	$5.41
Conservation	$13.03	$12.79	$12.47	$12.17
Total billed	$66,971.42	$63,375.45	$63,564.87	$53,506.63
Amount paid	$0.00	$63,375.45	$63,564.87	$53,506.63
Interest	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Penalty	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Balance	**$66,971.42**	**$0.00**	**$0.00**	**$0.00**

V. THE PRESENT SIMPLIFIED ANALYSIS FRAMEWORK

It is clear that any person using an analysis framework on smart city projects will need to account for many complex factors. This issue has been documented by other authors, who correctly point out that even deriving a basic notion of what "value" is for a smart city project is subjective. This is because different stakeholders, such as end-users and professionals, will arrive at different definitions of "added value" of the solution [29].

To make determinations of added value even more complicated, the impact of time, needs to be addressed. While measuring impact is a useful measure to derive for a municipal project, it is only possible to take a snapshot in time of impact [13]. This limitation can be compensated for, however, by analyzing the various contracts and controlling agreements of a public-private partnership to determine the obligations each stakeholder has. These agreements also account for controlling policies and regulation for the duration of the project. The snapshot dilemma is eliminated through this approach because the underlying agreements are applicable for the duration of the project.

A linear model based on the information presented above is now described. Taxpayers fund governments, which then allocate them to projects. The model is expressed as a cashflow diagram in Figure 5.

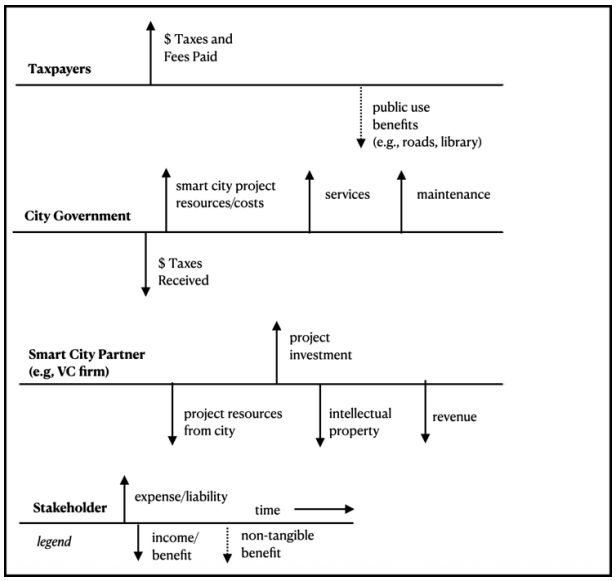

Figure 4. Costs and benefits to public-private partnerships can be understood as simple inputs and outputs.

VI. A New Framework

Other authors propose a template for characterizing the value proposition a smart city project provides the public from a technical, or systems perspective. The concept of a value chain typically defined in the business context is employed to capture the variety of ways that a project would presume to serve a public good [30]. Relying heavily on a systems approach to the exclusion of basic human needs and desires, however, risks alienating the population, or in a worst-case scenario treating the population as a "problem to be managed" [31].

An analysis framework that omits stakeholders or does not weigh the projects benefits against the stakeholders' individual obligations would blind an analyst to circumstances, writ-large, that could render the entire project useless to anyone. For example, a contractor who receives a grant to complete a smart city project has no obligation to demonstrate additional value to the taxpayers who indirectly funded the project. This creates an imbalance of responsibility where the taxpayer can be sanctioned for not paying taxes that support the project, while the grant recipient has no apparent consequence of failing other than a poor reputation and perhaps loss of future opportunities. This would be permitted in a scenario where the needs of the grant recipient were considered to the exclusion of the taxpayer's obligations to fund the project.

With that in mind, the simplified model above is now updated to incorporate the notion of stakeholder obligations to a public-private partnership. When incorporated into an analytical framework, assigning value based on obligations,

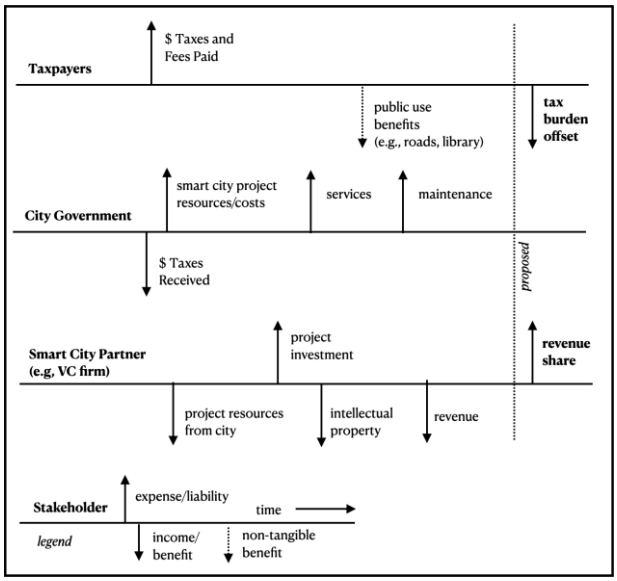

Figure 5. A revenue share that offsets tax burdens is one of many options.

or consequences, identifying an objective value proposition for each stakeholder is a straightforward exercise. Table V presents an example.

TABLE V. Project values change based on partnership structure.

Stakeholder	Project. Name	Value Proposition	Obligations	Value Metric
Taxpayers	Smart Sensors	none	Tax payments required.	0
City Government	"	publicity	Grants, loan guarantees, office space	20
Technology Provider	"	sales	provide smart sensors	50
Smart City Startup	"	patents	fund 20% of project costs	80
Taxpayers	Fiber infrastructure	Available service	Optionally subscribe to internet	80
City Government	"	Increased tax base	Grants, loan guarantees, office space	60
Technology Provider	"	sales	Install fiber	50
Smart City Startup	"	patents	fund 50% of project costs	20

In Table V, there are two projects and the same set of stakeholders for each project. In the first project "Smart Sensors" the project has no value to taxpayers because they are required to fund a technology through taxes that they will not make direct use of. The second project, "Fiber

infrastructure", provides taxpayers an optional Internet service on the city's new fiber optic network. The project takes on a high value to the taxpayers because their payments for the service are only made when they are using the service. The value metric for the Smart City Startup, however, is decreased dramatically, because it is accepting the obligation of funding 50% with no guarantee that citizens will subscribe to the service. There is some value, however, to the Startup because it can recover costs through patent revenue.

VII. CONCLUSION AND FUTURE WORK

In this paper, we claim companies can leverage one city's smart city project to create intellectual property rights which empower them to collect revenue from other cities which, in turn, can impact local fiscal autonomy. We also claim that applying an obligation-based value metric to all stakeholders can help analysts to identify the overall effects of intellectual property assignment to a city's contractor. To demonstrate why and how this can be done, we pulled together a broad set of selected data and research from multiple disciplines that are in-scope for smart cities. Concrete examples are used to show how diverse topics intersect in the context of a public-private partnership, such as intellectual property rights, systems related topics, intergovernmental organizations, municipal governance, legal aspects, and even constitutional considerations. Simple flow diagrams are used to illustrate the application of a simple analysis framework that can capture the obligations and benefits each stakeholder is expected to receive in a smart city public-private partnership. We demonstrate that the objective information needed for such analysis can be extracted from the underlying agreements, laws, and policies that govern the public-private partnership. We then extended the analysis framework to include a mechanism by which the tax obligations of a city taxpayer could be offset by intellectual property revenue.

The framework and model presented aims to shift the narrative around smart city projects to account for the value proposition stakeholders receive, and to express that value proposition in terms of how consequential the project is to each one. The project documents, contracts, data, and other concrete information that memorializes the legal partnership can be utilized to objectively assess the obligations of each stakeholder, determine the value propositions, and assign a value metric based both.

A path to future work is also implied by the analytic framework and model presented. This approach is expected to scale to projects of any size, and in general the work will simply increase with the amount of information available about the project.

Using this framework to analyze real projects is suggested as a future project.

REFERENCES

[1] T. S. Woodson, "Public private partnerships and emerging technologies: A look at nanomedicine for diseases of poverty, Research Policy," vol. 45, issue 7, 2016, pp. 1410-1418, ISSN 0048-7333, https://doi.org/10.1016/j.respol.2016.04.005.

[2] N. Beermann, "Legal Mechanisms of Public-Private Partnerships: Promoting Economic Development or Benefiting Corporate Welfare?," 23 SEATTLE U. L. REV. 175, 1999.

[3] Seattle University Law Review. (Online). https://digitalcommons.law.seattleu.edu/sulr/. [retrieved: December 2024].

[4] The City of Seattle Website. (Online). https://www.seattle.gov/. [retrieved: November 2024].

[5] King County, Washington, USA Website. (Online). https://kingcounty.gov/. [retrieved: November 2024].

[6] The American Journal of Comparative Law. (Online). https://academic.oup.com/ajcl. [retrieved: February 2025].

[7] Elsiver. (Online). https://elsevier.com. [retrieved: November 2024].

[8] Taylor and Francis Online. (Online). https://www.tandfonline.com/. [retrieved: January 2025].

[9] World Economic Forum. (Online). https://www.weforum.org . [retrieved: January 2025].

[10] US Census Bureau. (Online). https://www.census.gov. [retrieved: February 2025].

[11] P. Jacobsen, "Leveraging PPPs for Smart City Infrastructure," World Bank. [Online]. Available from https://www.gfdrr.org/sites/default/files/D3_CaseStudy16_PaulJacobson_PPP_Smart_cities.original.1531294896.pdf. [retrieved: February 2025].

[12] A. Voorwinden, "The privatised city: technology and public-private partnerships in the smart city," Law, Innovation and Technology, 13(2), pp. 439–463. https://doi.org/10.1080/17579961.2021.1977213.

[13] L. Berntzen, "Measuring the Impact of eGovernment Services," The Eighth International Conference on Digital Society (ICDS 2014) IARIA, March 2014, pp 54-58, ISSN 2307-3956, ISBN: 978-1-61208-324-7

[14] D. Custos and J Reitz, "Public-Private Partnerships," The American Journal of Comparative Law, vol. 58, Issue suppl_1, Supplement 2010, pp. 555–584, https://doi.org/10.5131/ajcl.2009.0037.

[15] M. Buso, M. Moretto, and D. Zormpas, "Excess returns in Public-Private Partnerships: Do governments pay too much?," Economic Modelling, vol. 102, 2021, 105586, ISSN 0264-9993, https://doi.org/10.1016/j.econmod.2021.105586.

[16] C. Kalleya, A. Purnomo, E. D. Madyatmadja, and Meiryani, M. Karmagatri, "Smart City Applications: A Patent Landscape Exploration," Procedia Computer Science, vol. 227, 2023, pp. 981-989, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.10.607.

[17] P. Silal, A. Jha, and D. Saha, "Managing E-Government Development for Reducing Corruption via Effective Policymaking: Emerical Evidences from Cross-Country Analysis," The Thirteenth International Conference on Digital Society (ICDS 2019) IARIA, February 2019, pp 1-7, ISSN 2307-3956, ISBN: 978-1-61208-685-9.

[18] R. M. Schomaker, "Conceptualizing Corruption in Public Private Partnerships," Public Organiz Rev 20, pp. 807–820, 2020. https://doi.org/10.1007/s11115-020-00473-6.

[19] M. Scutella, C. Plewa, and C. Reaiche, "Customizing eGovernment Support Services: A Value Co-Creation Perspective," The Fourteenth International Conference on Digital Society (ICDS 2020) IARIA, November 2020, pp 30-33, ISSN 2307-3956, ISBN: 978-1-61208-760-3.

[20] T. Cellucci and J. Grove, "Leveraging Public-Private Partnership Models and the Free Market System to Increase the Speed-of-Execution of High-Impact Solutions throughout State and Local Governments," US Homeland Security Science and Technology. [Online]. Available from: https://www.dhs.gov/xlibrary/assets/st-leveraging-partnerships-for-state-and-local-governments-August2011.pdf. [retrieved: February 2025].

[21] Seattle AI Incubator Announcement. [Online] https://harrell.seattle.gov/2025/03/27/mayor-bruce-harrell-and-city-of-seattle-launch-groundbreaking-ai-incubator-to-propel-the-next-generation-of-ai-entrepreneurs/. [retrieved: March 2025].

[22] World Economic Forum. (Online). https://www.weforum.org/impact/smart-cities-governance-alliance/ [retrieved: February 2025].

[23] WEF C40 Cities, ARUP, and University of Leeds, “The Future of Urban Consumption In a 1.5°C World,” World Economic Forum. (Online). https://www.c40.org/wp-content/uploads/2023/04/2270_C40_CBE_MainReport_250719.original-compressed-1-2.pdf [retrieved: March 2020].

[24] King County Tax Foreclosures. (Online) https://kingcounty.gov/en/dept/executive-services/buildings-property/treasury-operations/tax-foreclosures [retrieved: February 2025].

[25] King County Parcel Viewer. (Online) https://gismaps.kingcounty.gov/parcelviewer2/. [retrieved: February 2025].

[26] Columbia Telecommunications Corporation, “A Plan For Facilitating Equitable Access to Wireless Broadband Services in Seattle,” City of Seattle. [Online]. Available from https://www.seattle.gov/documents/departments/broadband/facilitatingequitableaccesstowirelessbroadbandservicesinseattlectcreport2017.pdf. [retrieved: June 2017].

[27] Y. Erica, J. Walczak, “State and Local Tax Burdens, Calendar Year 2022,” Tax Foundation. (Online) https://taxfoundation.org/data/all/state/tax-burden-by-state-2022/ [retrieved: June 2024].

[28] T. Szewc and S. Rubisz, “Intellectual Property Issues in Managing a Smart City,” Scientific Papers of Silesian University of Technology – Organization and Management Series, iss. 168, Available at SSRN: https://ssrn.com/abstract=4351515 or http://dx.doi.org/10.2139/ssrn.4351515.

[29] M. Hartog and B. Mulder, “Preconditions for the Structural Deployment of (Digital) Technology for Healthcare in a Participatory Society: Validation of methodological and practical challenges,” The Twelfth International Conference on Digital Society (ICDS 2018) IARIA, March 2018, pp 14-16, ISSN 2307-3956, ISBN: 978-1-61208-615-6.

[30] C. Pfister, S. Haller, and E. Klein, “Towards a Smart City Blueprint Template,” The Thirteenth International Conference on Digital Society (ICDS 2019) IARIA, Februaryt 2019, pp 30-36, ISSN 2307-3956, ISBN: 978-1-61208-685-9.

[31] G. Halegoua, “Smart Cities,” Chapter 4; MIT Press: Cambridge, MA, USA, 2020.

Consequences of the EU Data Act and the EU General Data Protection Regulation to the Modern Smart Home Data Economy

Paul Seidel, Felix Fischer, Dirk Labudde
Faculty Applied Computer Sciences and Biosciences
Hochschule Mittweida University of Applied Sciences
Mittweida, Germany
e-mail: {seidel6 | fische11 | labudde}@hs-mittweida.de

***Abstract*—The entry into force of the European Union (EU) Data Act 2024 creates new opportunities for the European data market, but also new challenges. One such challenge is the parallel application of the EU General Data Protection Regulation (GDPR). It is, therefore, necessary to analyse these two regulations and their consequences for the players in the Smart Home sector. To this end, the Smart Home sector and its relevant players are analysed and potential conflicts between the EU Data Act and the EU GDPR are identified. One such conflict arises in the management of personal data from multi-user environments. In the Smart Home in particular, several users share different devices, such as smart TVs, and thus generate mixed data sets that are not compliant with the regulation. If a member of the user community wishes to transfer their data to a third party in accordance with their rights guaranteed by the EU Data Act, the third party must be able to ensure that the transferred data are not also the personal data of another user.**

Keywords-EU data act, GDPR, contradiction, smart home.

I. Introduction

Increasing digitalisation and the steady expansion of data-based business models have placed the so-called data economy at the heart of economic and technological developments. Data are regarded as the new oil of the 21st century [1] and are essential for value creation in areas such as machine learning, whose economic potential through generative models has recently been estimated at several trillion dollars [2, p. 3]. This makes the regulation and utilisation of data a key challenge for modern economies.

The Smart Home plays a central role in this data economy, as connected devices generate a wide range of data that can benefit both users through better services and manufacturers through commercial exploitation [3]. However, currently European consumers often do not have access to their data, which hampers innovation and competition [4]. The European Union (EU) Data Act aims to redress this imbalance by granting users extensive rights to their data, including real-time access to device-generated data [5, Art. 3]. In addition to the General Data Protection Regulation (GDPR), which already provides for the right to data portability [6, Art. 12 para. 3], the Data Act aims to promote competition and interoperability, for example through 'cloud switching' and access to manufacturer data for repair services [5, Recital 78]. However, at the same time, there is a tension between the two regulations. While the Data Act also requires the transfer of mixed data sets, the GDPR prioritises the protection of personal data and prescribes strict sanctions for violations [5, Art. 1 para. 5]. This leads to legal uncertainties, particularly in the Smart Home, where mixed data sets are often created. With the EU Data Act becoming applicable law in September 2025, this issue is becoming increasingly relevant and requires technical solutions to take into account both regulatory requirements and the technical innovation potential.

The urgency of this study arises from that recent entry into force of the EU Data Act, which significantly reshapes the regulatory landscape for data access and sharing in Europe. Particularly in Smart Homes, where multiple users often interact with interconnected devices and generate mixed datasets, the practical application of the Data Act introduces tensions. This study examines these tensions, focusing on the legal and technical challenges of managing personal data in multi-user environments and ensuring regulatory compliance. The specific designs and implementations of the technical and legal solutions to these challenges are beyond the scope of this study.

After this introduction, the key stakeholders and challenges in the Smart Home sector are discussed in Section II, focusing on their interests and the inherent problems in this environment. Also in Section II, the concept of the Smart Home is defined, and the roles of relevant stakeholders are explored. Section III then examines the challenges posed by the data economy in Smart Homes, particularly data protection issues and power asymmetries between consumers and service providers. In Section IV, the EU Data Act and the GDPR are analyzed, providing an overview of both regulations, highlighting potential conflicts, and assessing their implications for the Smart Home sector. Finally, the paper concludes with a summary of findings and directions for future work in Section V.

II. Stakeholders and Problems in the Smart Home

The Smart Home sector is a central component of the modern data economy, in which consumers, device manufacturers and service providers operate in a complex network of economic and regulatory relationships. In order to better understand the opportunities and risks of this sector, a comprehensive analysis of the players involved and their interests is required. Therefore, the basic concepts and functioning of the Smart Home, as well as the roles of the relevant players, are first examined, and the potentials and risks arising from

the use of the data generated in the Smart Home are analyzed. The central challenges of the data economy in the Smart Home context are then analysed, with a focus on data protection problems, economic effects and power imbalances between users and providers.

A. Smart Home - Definition and concept

The Smart Home is based on the technologies of Embedded Systems and the Internet of Things (IoT). Embedded Systems are specialised, integrated computer systems designed to automate and simplify the functionalities of the host device [7, ch. 1]. Networking via technologies such as IEEE 802.11, usually referred to as Wireless Local Area Network (WLAN), or Bluetooth creates the IoT, which enables communication between devices and their real-time interaction [8].

In the Smart Home, this IoT architecture is used to network household appliances and automate everyday processes [9]. The aim is to increase comfort, safety and efficiency, for example through smart thermostats that optimise energy consumption based on the habits of the residents [10][11].

An overview of the terms Embedded Systems, Internet of Things and Smart Home is summarised in Table I.

TABLE I. DEFINITION OF TERMS: EMBEDDED SYSTEMS; IOT; SMART HOME

Term	Definition	Examples
Embedded systems	mechanical and electrical systems with integrated software	modern cars, cash register systems, ATMs
Internet of Things (IoT)	interconnected embedded systems	Industry 4.0, car-to-car communication
Smart Home	IoT systems in home automation	vacuum/mopping robots, SmartTVs

The networking of Smart Home devices opens up numerous opportunities to make everyday life easier and to organise processes more efficiently by networking various household appliances. For example, the data collected can be used to increase comfort and energy efficiency in households [12]. In the healthcare sector in particular, wearables, such as smart watches offer the possibility of recognising medical emergencies, such as strokes or heart attacks at an early stage, enabling faster and potentially life-saving interventions [13][14]. Home automation also benefits the environment, as intelligent control systems can optimise the energy consumption of appliances. Automated adjustment of heating, lighting and other systems not only reduces costs for residents, but also helps to reduce the ecological footprint [15][16]. An illustrative example is the automatic switch-off of radiators as soon as windows are opened [17].

Smart home data is also used to improve building security. Intelligent monitoring systems can recognise break-ins at an early stage and initiate preventative measures. In addition to traditional dangers, such as burglaries, invisible risks, such as voltage peaks, critical air conditions or structural damage to buildings can also be detected and communicated to the residents [18, p. 7][19][20]. In addition, personalised functions, such as alarm clocks, music or news, enrich daily life by being tailored to the individual preferences of residents. The use of modern Artificial Intelligence (AI) technologies makes it possible to analyse the collected data and turn it into meaningful automated decisions [21][22].

The symbiosis between AI and Smart Home technologies mutually reinforces both areas. AI relies on using large amounts of data to develop powerful models, while Smart Home devices continuously generate such data [23][24]. This creates a market in which data trading plays a central role. Companies that rely on AI-supported solutions buy the necessary data, while the owners of this data can monetise it. This creates an economic incentive, especially for companies without the technical resources to utilise their own data [5, Recital 19].

Networked systems also offer potential at a societal level, for example in public health management. During the COVID-19 pandemic, it became clear how valuable data-driven systems can be in tracing chains of contact [25]. Applications such as the *Corona-Warn-App* [26] helped to break chains of infection and slow down the spread of the virus. At the same time, however, the collection and processing of sensitive data raises questions about the protection of privacy. While the pandemic has demonstrated the benefits of such technologies, it has also revealed the risks of large-scale data collection and storage. Sensitive information on health, behaviour and habits could be exposed or misused by cyberattacks, causing considerable harm to the individuals concerned [27, pp. 11]. Weighing up the benefits of data-driven innovations against the risks to privacy and security therefore remains a key challenge for the Smart Home data economy.

B. Relevant stakeholders and interests

To analyze the dynamics within the Smart Home ecosystem, stakeholders were grouped along two dimensions: their level of access to data and their technical know-how to generate value from it. Four central stakeholder groups (SG) operate in the Smart Home sector. The relationships between the stakeholder groups are shown graphically in Figure 1.

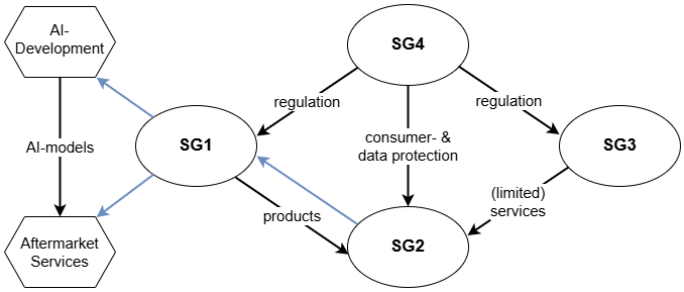

Figure 1. Relationship diagram of the actors in the Smart Home and IoT Legend: SG1 - Gatekeepers; SG2 - Users; SG3 - Aftermarket service providers; SG4 - Legislators and institutions; Data relations in blue.

SG1: Gatekeeper Technology companies such as Amazon and Google dominate the market by manufacturing devices

and utilising data. Their focus is on increasing profits, often at the expense of data protection and despite strict regulations such as the GDPR [28][29]. As gatekeepers, they control the data that is created on devices produced by them. Therefore, they have a significant influence on the market and competition [30]. Gatekeepers typically have both privileged access to user data and the technical expertise to extract economic and strategic value from it.

SG2: Users Consumers benefit from automation and innovation, but are also the main source of data. Entertainment Systems, such as Smart TVs are the most popular among users, while building security and automation solutions are less common [31]. User priorities are security and convenience [32]. Customers and private users have limited technical capabilities and often only partial access to the data they generate.

SG3: Aftermarket service providers Companies offering repair services and cloud providers are heavily dependent on gatekeepers as they often lack access to critical data. They may have the technical know-how but face barriers in data access due to platform control and interoperability issues. This hampers innovation and fair competition [33].

SG4: Legislators and institutions Legislation, particularly at EU level, is aimed at data protection, consumer protection and a fair data market. Data from Smart Home systems could also be used in crises, such as pandemics or natural disasters [34].

III. Challenges of the data economy in the Smart Home

The data economy faces significant economic and legal hurdles, particularly in the Smart Home sector. A central problem are the gatekeepers - powerful technology companies that primarily operate outside the EU and exert considerable influence on the global flow of data. Their dominance makes it difficult to enforce European data protection regulations [35] and manifests itself in various power asymmetries vis-à-vis their customers. The trade in personal data and the data protection-compliant processing of this data pose further challenges, which can result in financial losses that threaten the existence of small and medium-sized companies in particular if the applicable regulations are not observed.

A. Data protection issues in the Smart Home

The data generated by Smart Home devices often contains sensitive and sensitive information about users and their everyday habits [5][36]. IoT technologies are expected to have a significant impact on the healthcare sector in particular, which further emphasises the sensitivity of this data [12]. Manufacturers of Smart Home devices and services have a significant influence on what data is collected and shared, while consumers are often insufficiently informed about the scope and storage of this data [37]. Without technical expertise, it is almost impossible for consumers to verify the accuracy of the specified data processing modalities and their control over the data they generate is severely limited [36]. In many cases, the only option available to users with data protection concerns is to opt out of the product or service.

Intelligent voice assistants are a particularly clear example of the lack of transparency in data processing. These systems require permanent monitoring of the acoustic environment in order to be able to react to trigger phrases [37]. Although data is only transmitted after a keyword has been recognised, voice assistants can be activated unintentionally, e.g. by similar-sounding phrases, whereby data is transmitted without the explicit request of the user [38]. Users are often left in the dark about the scope of the data collected, as detailed information can only be requested on their own initiative and in accordance with the applicable data protection laws, such as the GDPR. In addition, this data is usually not processed locally, but decentralised on the providers' cloud servers [39], which severely restricts the user's control over the transfer and processing of data.

To better understand the regulatory challenges in Smart Home environments, it is required to distinguish between different types of data and their sources. Table II classifies Smart Home data along two dimensions: the nature of the data (personal vs. non-personal) and its origin (individual users or shared use).

TABLE II. Classification and Examples of Smart Home Data by User and Type

Data Type	User 1	User 2	Shared
Personal Data	voice assistant queries, health data	TV preferences, fitness data	shared calendar, living room camera footage
Non-Personal Data	generic device usage statistics (e.g. light switches)	app update logs, battery charging cycles	energy consumption, network diagnostics

This classification in Table II highlights the complexity of data governance in multi-user settings, where personal and non-personal data often coexist and overlap, raising important questions about ownership and access rights.

The decision on how to handle the collected data often lies with the manufacturers, while the users, despite legal requirements such as [6, Art. 12-14], have no direct insight into or control over access to their data. In many cases, this data is sold to third parties or used by the provider to develop new services, often without the express consent of the user [37]. Even after the use of Smart Home devices, many providers retain the collected data, which increases the risk of future misuse or disclosure through security incidents [40].

Consumers are also dependent on manufacturers and service providers in their ability to protect their data, as they store the data in cloud systems [39][41]. Data protection-friendly functions, such as encryption or multi-factor authentication are often missing and can only be implemented by the manufacturer [37]. Particularly in connection with identifying data, such as payment or geolocation data, which by its very nature can be assigned to individuals, the security of this personal data depends largely on the security precautions taken

by the cloud provider. In the event of a data leak, serious consequences, such as identity theft or financial damage can occur [42]. For companies that rely on networked devices, data protection incidents can also lead to a loss of sensitive business secrets, which harbours considerable economic risks [43].

There is a further risk in the second-hand trade for IoT and Smart Home devices. Due to the frequent lack of user interfaces on embedded devices, resetting used devices to factory settings is difficult and can result in the previous owner's personal data remaining on the device [44]. The new owner could unintentionally or maliciously gain access to this data or use functions that are linked to the previous owner's account.

B. Power asymmetries between consumers and service providers

In the course of the increasing networking of household appliances and the data-driven economy, power asymmetries between consumers and service providers (specifically SG1 'gatekeepers') are becoming ever more apparent. These result not only from the technical complexity, but also from the legal and economic conditions, which restrict consumers' scope for action and make access to the data they generate more difficult.

A central feature of these asymmetries are non-negotiable user agreements dictated by the provider. Particularly in the area of Smart Home technologies, providers impose opaque contractual terms and conditions [36], which can usually only be accepted by accepting or waiving the service. These often contain clauses that grant extensive rights of use to personal data or severely limit the provider's liability [45]. The exact scope of data use often remains opaque, which increases consumer mistrust [36]. The lack of transparency about data processing and the invisibility of processes that take place in remote data centres [39] further increase this scepticism. Access to and management of personal data often takes place via complex, less user-friendly platforms [46], which makes it difficult for many users to exercise their rights under the GDPR.

A particularly clear example of this power asymmetry is Amazon's Alexa voice assistant system. Here, the consumer has little control over the extent of data usage, as these processes are decentralised and hidden [47]. Users are dependent on a continuous connection to the cloud in order to use the service [48]. This increases dependency on the provider and makes it difficult to switch to alternative providers.

In addition, the lack of interoperability of cloud services makes it difficult to switch between different providers, as many systems are proprietary [49]. The repair options for Smart Home devices are also limited, as often only the manufacturer can carry out repairs [50].

These structural imbalances are leading to a loss of trust among consumers, who are increasingly trying to remove their data from the providers' streams. Data protection-oriented technologies such as Brave or the Tor browser, as well as specialised 'data removal services', are therefore gaining in importance [51]. This loss of trust, especially with regard to the technical security of networked devices, could damage the Smart Home sector in the long term as the value of the data collected decreases [31].

IV. EU Data Act and GDPR in the Smart Home

In this section, two central and widely applicable EU regulations with great relevance for the Smart Home and the data generated therein are analysed: the GDPR and the EU Data Act. These regulations aim to regulate the handling of personal and machine-generated data, strengthen consumer rights and address the issues analysed in Section II, such as data protection problems and power asymmetries between service providers and users.

Together with other legislative measures, for instance the EU Digital Markets Act, the EU Digital Services Act and the EU Data Governance Act, they form the basis of the European Commission's digital strategy.

A. Overview of the EU Data Act

The EU Data Act (EU Regulation 2023/2854) is a central element of the European data strategy and regulates access to and use of the generated data collected by digital technologies such as Smart Home devices and cloud computing. The regulation was adopted in November 2023, has been in force since the beginning of 2024 and will be applicable law from September 2025 [52]. The aim is to ensure fair access to data and a fair distribution of data between different market players [4].

Manufacturers and service providers (data owners) are obliged to grant users prompt access to their generated data [5, Art. 3 para. 1]. This also includes the right to pass the data on to third-party providers who can use it to develop innovative products and services [5, Art. 5]. In the Smart Home sector in particular, this should help to ensure that not only large companies benefit from the data economy, but also smaller players [5, Recital 30 & 32].

The processing of personal data remains subject to the provisions of the GDPR, which takes precedence in the event of conflicts [5, Art. 1 para. 5]. The regulation is intended to give users more control over their data, as many consumers or companies do not have the resources to utilise the full economic value of their data themselves [5, Recital 3 & 19 & 40]. One example of implementation is the management of data by virtual assistants. These collect information about Smart Home users, for example to control heating or lighting. The EU Data Act enables users to manage this data and pass it on to third-party providers, which could give rise to new smart assistance systems [5, Recital 22].

In order to curb the market dominance of large platforms, gatekeeper companies defined under the EU Digital Markets Act may not use data that does not originate from their own devices [5, Art. 5 para. 3]. This is intended to prevent excessive concentration of market power [53][54]. In addition, the EU Data Act is intended to help better manage such public emergencies as pandemics or cyberattacks. In such cases, public authorities can request relevant data, whereby

the modalities are clearly defined and companies may be compensated for providing it [5, Art. 14 & 17].

Figure 1 can thus be extended to Figure 2.

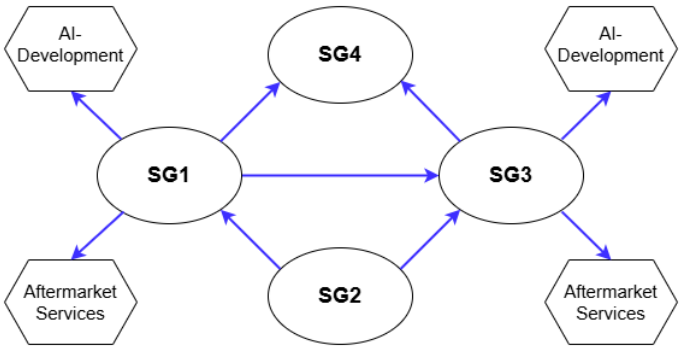

Figure 2. In terms of the EU Data Act, modified relationship diagram of the actors in the Smart Home and IoT area from Figure 1
Legend: SG1 - Gatekeepers; SG2 - Users; SG3 - Aftermarket service providers; SG4 - Legislators and institutions; Data relations in blue.

With the EU Data Act becoming applicable law, data that was previously exclusively accessible to gatekeepers (SG1) will be available to all authorised interested parties (see Figure 2). This enables European companies (SG3) to develop their own data-based services, while public authorities (SG4) can manage crises more efficiently.

However, the extended availability of data harbours security risks. Data owners are responsible for securing access and data, but can use modern security measures, for example encryption or smart contracts [5, Art. 3 para. 1, Art. 11 para. 1]. Users and recipients may only adapt these measures with the consent of the data controller without being restricted in their use of data.

Another key issue is cloud switching: users should be able to switch more easily between cloud providers, such as Amazon Web Services (AWS) or Microsoft Azure. Providers must support customers when switching [5, Art. 25 para. 2a], ensure business continuity and, from 2027, no longer charge fees for the move [5, Art. 29]. This incentivises structured, machine-readable data formats and technologies for smooth data migration [5, Recital 78 & 84].

Smart contracts are proposed as possible interfaces for automated data transfers to enable the secure and traceable execution of agreements [5, Art. 2 para. 39]. The EU Data Act requires high security standards, protection against manipulation and audit-proof archiving of the generated data [5, Art. 36]. Providers must regularly submit declarations of conformity to prove compliance with the regulations.

The regulation also emphasises security in critical infrastructures, for example energy and water supply [5, Recital 14]. In addition to the GDPR, security checks and measures such as pentests and encryption are also to be performed and implemented for non-personal data [5, Recital 102].

For implementation, national authorities are to be appointed or established to impose effective sanctions in the event of violations [5, Art. 37 & 40]. If several authorities are involved, a data coordinator will be appointed for coordination, while GDPR supervisory authorities will remain responsible for personal data [5, Art. 37 para. 3].

The EU Data Act addresses the asymmetric market power in the IoT sector in favour of users and strengthens competition [55, p. 26]. However, there are challenges: User consent remains a weak point, and interactions with the GDPR are still unclear [55, pp. 23]. Further legal and technical coordination is required in order to realise the full benefits of the EU Data Act.

B. Overview of the GDPR

The General Data Protection Regulation (GDPR) has been in force as binding law in the EU since 2018 and aims to ensure the protection of personal data [6]. It was introduced in response to increasing digitalisation and the growing amount of data collected [56]. Large tech companies in particular benefit from analysing and using such data [6, Recital 6].

A clear legal framework has been created to regulate data processing, which obliges companies to meet high standards and provides for sanctions in the event of violations [6, Recital 7]. In practice, however, there are difficulties with enforcement, particularly in cross-border cases [35].

The GDPR defines key terms such as *personal data*, *processing* and *profiling* [6, Art 4] and sets out binding principles for the handling of personal data. These include lawfulness, purpose limitation, data minimisation and accountability [6, Art. 5].

Data subjects have extensive rights, including rights to information, access and erasure [6, Art. 13-17]. Data controllers must ensure that these rights are respected and are obliged to appoint data protection officers and report data breaches within 72 hours [6, Art. 24 & 33].

An evaluation of the GDPR from 2024 emphasises the central role of data protection officers, especially for small and medium-sized enterprises [57, p. 3]. In addition, the regulation should be made less bureaucratic to enable more efficient and risk-based implementation [57, pp. 4]. Digital service providers should also be more closely integrated into the obligations of the GDPR in order to improve users' control over their data [57, pp. 5].

C. Comparison and conflicts between the two regulations

The GDPR and the EU Data Act have different priorities, but are not fundamentally contradictory. While the GDPR prioritises the protection of personal data and consumer protection, the EU Data Act focuses on promoting a data-driven economy and facilitating access to non-personal data [58]. Both sets of regulations share the goal of supporting the free movement of data within the EU by striving for a balance between data protection and the commercial use of data.

Both the GDPR and the EU Data Act contain provisions for crisis situations: While the EU Data Act permits the provision of relevant data, the GDPR authorises public bodies to process personal data in certain cases [6, Art. 2 para. 2d][5, Art. pp. 14]. These regulations can be helpful in the context of pandemics or disaster management, for example, but raise

questions in the area of law enforcement and anti-terrorism measures. The centralised availability of data via data traders could also open up new opportunities for fighting crime, the effects of which need to be investigated further.

A central area of tension arises when networked devices generate personal data, as the EU Data Act makes it clear that it must not affect the GDPR and takes second place to it in the event of a conflict [5, Recital 34][5, Art. 1 para. 5]. This becomes particularly problematic in multi-user scenarios: A single user could share or sell data that also affects other people without their consent. This would be a violation of the GDPR [6, Art. 13]. At the same time, the EU Data Act obliges providers to provide non-personal data [5, Art. 3], which creates a legal dilemma: A refusal could violate the EU Data Act, a disclosure could violate the GDPR.

The distinction between personal and non-personal data poses a further challenge, especially in the case of mixed data sets. The EU Data Act requires a clear classification in order to provide commercially usable data, while the GDPR comprehensively protects personal data [5, Art. 3][6, Art. 18]. It is particularly critical that originally non-personal data can become personal information through correlation or analytical procedures [59, p. 6 & 16][60]. This could lead to data protection provisions being circumvented through clever contractual constructions.

The practical implementation of both sets of regulations also poses challenges for companies. Small and medium-sized enterprises in particular are confronted with considerable bureaucratic effort due to the parallel requirements of the GDPR and the EU Data Act, which ties up resources and can inhibit innovation processes [57][58].

Approaches such as anonymisation or selective data sharing are being discussed to resolve these conflicts, although their technical feasibility and effectiveness remain questionable. A more precise regulation on the separation of personal and non-personal data as well as a clear legal handling of multi-user scenarios are necessary in order to make the coexistence of both sets of rules practicable [5, Recital 7].

D. Relevance for the Smart Home

Smart home devices, as part of the IoT, collect a lot of data in the home environment and are explicitly mentioned in the EU Data Act [5, Recital 23]. Currently, however, these systems are often limited by incompatibilities, while users find it difficult to access their own data [33][61]. The EU Data Act is intended to counteract this by promoting better data accessibility and interoperability between manufacturers [5, Recital 32]. This not only enables personalised services, but also facilitates the repair of defective devices through improved data access [5, Recital 32].

As considerable amounts of data are generated in the Smart Home, these are not only of economic interest to users, but also to companies. The EU Data Act obliges providers to make this data available - both to consumers and to third parties, including competitors [5, Recital 39].

The data collected affects many areas of life, from health to entertainment [62], and offers both individual and economic benefits [5, Recital 64]. At the same time, they are often personal [36] and are therefore subject to the GDPR, which creates data protection risks, especially through the detailed recording of user behaviour [36].

Heino et al. [36] describe four central data protection problems in the Smart Home:

(1) Unclear legal scope of application,
(2) Lack of transparency in data processing,
(3) Preset data collection with opt-out instead of opt-in and
(4) Uncertainties regarding retention periods. Added to this is the principle of data minimisation, which conflicts with the usefulness of many devices, as more data often means better functionality [59, p. 15][63, p. 3].

Following our analysis, we would expand this list based on the differences between the kinds of data generated in the smart home, as described in Table II:

(5) Blurred boundaries between personal and non-personal data, especially in shared or mixed-use contexts,
(6) Ambiguity in attributing data to specific individuals in multi-user environments,
(7) Unclear responsibilities for data governance when data is co-generated or shared across devices and users,
(8) Conflicts between user rights under the Data Act (e.g., data portability) and the privacy rights of other users under the GDPR.

Since the GDPR came into force, users in countries with GDPR-compliant legislature are increasingly aware of data security risks and have a higher perceived level of control [64]. The multi-user operation of Smart Home devices makes GDPR compliance more difficult. In households, several people share devices, which makes it challenging to clearly assign and control personal data. A flexible solution is needed to combine data protection and usability.

V. Conclusion and Future work

The Smart Home has been identified as an increasingly relevant component of the data economy, in which the residents of a networked living space generate a large amount of data through their use of intelligent devices. This data offers significant potential for new services, such as personalised energy management systems or health-applications, but also creates risks. These include data protection problems, security gaps and the possibility of commercial exploitation of user data by third parties.

The Smart Home sector is characterised by a wide range of actors, including manufacturers of IoT devices, service providers, public authorities and consumers themselves. These players often pursue divergent interests: While providers primarily aim to monetise user data, consumers demand stronger data protection measures and easy ways to control their data. The power asymmetries between large technology providers and their customers or small to medium-sized enterprises were identified as particularly problematic,

as they hinder innovation and competition in the sector.

The forthcoming applicability of the EU Data Act and the existing requirements of the GDPR are having a significant impact on the Smart Home sector. The EU Data Act addresses the current power asymmetry by facilitating data access for data-generating customers and third-party providers, thereby promoting competition and innovation.

The GDPR, on the other hand, emphasises the protection of personal data and defines strict requirements for its processing. In combination, these two regulations create a complex legal framework and therefore pose considerable challenges. Conflicting objectives arise, particularly in the case of mixed data sets that contain both personal and non-personal information of several users: while the EU Data Act requires the release of non-personal data, the GDPR demands strict protective measures for personal data. This leads to uncertainties as to how the two regulations can be harmonised without violating data protection regulations and fearing sanctions. If such uncertainties are not adequately addressed, the Data Act may have the opposite of its intended effect and hinder innovation through diminished customer acceptance and reduced trust in data-driven services.

In view of regulatory developments and the increasing spread of Smart Home technologies, several relevant research questions arise. One key issue is the practical implementation of the EU Data Act in the area of conflict with the GDPR, particularly with regard to the separation of personal and non-personal data within mixed data sets. There is a need for further clarification here to ensure that both data protection requirements and economic interests are adequately taken into account.

Another research approach is the development of technical solutions for more data protection and data sovereignty in the Smart Home. Approaches such as federated learning or edge computing could help to make data processing more decentralised in order to reduce security risks and power asymmetries. There is also a need for further research into how users can obtain intuitive and effective control mechanisms over their data without compromising the user-friendliness of Smart Home systems.

Finally, the economic and social impact of the new regulations must also be analysed. It remains to be seen to what extent the EU Data Act will actually promote competition in the Smart Home market or whether new challenges will arise due to regulatory uncertainties. Further research could focus on what adjustments the industry needs to make in order to fulfil the legal requirements and develop innovative, data protection-compliant business models.

Acknowledgement

This paper was funded by the European Union and the Free State of Saxony (Germany).

Kofinanziert von der Europäischen Union

Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.

References

[1] M. Szczepanski, “Is data the new oil?” accessed: 09.04.2025, Jan. 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf.

[2] M. Chui et al., “The economic potential of generative ai - the next productivity frontier,” accessed: 09.04.2025, 2023. [Online]. Available: http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/14313/1/The-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf.

[3] Publications Office of the European Union, “Data act — factsheet,” accessed: 09.04.2025, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet.

[4] Council of the EU, “Data act: Council adopts new law on fair access to and use of data,” accessed: 09.04.2025, Nov. 2024. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/.

[5] European Parliament and Council of the EU, “Regulation (eu) 2023/2854 of the european parliament and of the council,” of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), *Official Journal of the European Union*, Dec. 2023, accessed: 09.04.2025.

[6] European Parliament and Council of the EU, “Regulation (eu) 2016/679 of the european parliament and of the council,” of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, May 2016, accessed: 09.04.2025.

[7] S. Heath, *Embedded Systems Design*. 2003, accessed: 09.04.2025, ISBN: 0-7506-5546-1.

[8] Federal Network Agency, “Federal network agency - internet of things,” accessed: 10.04.2025, Oct. 2024. [Online]. Available: https://web.archive.org/web/20250328092032/https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Internet/IoT/start.html.

[9] IBM, “Internet of Things,” May 2024. [Online]. Available: https://www.ibm.com/de-de/topics/internet-of-things.

[10] B. L. Risteska Stojkoska and K. V. Trivodaliev, “A review of internet of things for smart home: Challenges and solutions,” *Journal of Cleaner Production*, vol. 140, 2017, ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2016.10.006.

[11] L. Ferreira, T. Oliveira, and C. Neves, “Consumer’s intention to use and recommend smart home technologies: The role of environmental awareness,” *Energy*, vol. 263, p. 1, 2023, ISSN: 0360-5442. DOI: 10.1016/j.energy.2022.125814.

[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. DOI: 10.1109/COMST.2015.2444095.

[13] B.-O. Bat-Erdene and J. L. Saver, "Automatic acute stroke symptom detection and emergency medical systems alerting by mobile health technologies: A review," *Journal of Stroke and Cerebrovascular Diseases*, vol. 30, no. 7, p. 105 826, 2021, ISSN: 1532-8511. DOI: 10.1016/j.jstrokecerebrovasdis.2021.105826.

[14] NHLBI, "Novel sensor can detect a heart attack in just minutes," accessed: 09.04.2025, Oct. 2021. [Online]. Available: https://www.nhlbi.nih.gov/news/2021/novel-sensor-can-detect-heart-attack-just-minutes.

[15] M. Zehnder, H. Wache, H.-F. Witschel, D. Zanatta, and M. Rodriguez, "Energy saving in smart homes based on consumer behavior: A case study," in *2015 IEEE First International Smart Cities Conference (ISC2)*, 2015. DOI: 10.1109/ISC2.2015.7366231.

[16] A. Anvari-Moghaddam, H. Monsef, and A. Rahimi-Kian, "Optimal smart home energy management considering energy saving and a comfortable lifestyle," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 324–332, 2015. DOI: 10.1109/TSG.2014.2349352.

[17] Telecom, "Smarthome ideas: Heating control," accessed: 09.04.2025, Aug. 2024. [Online]. Available: https://web.archive.org/web/20240915162832/https://www.smarthome.de/ideen/smarte-heizungssteuerung.

[18] M. Bräuer, "Abus safety study 2023," 2023. [Online]. Available: https://www.abus.com/de/content/download/278385/file/ABUS-Sicherheitsstudie-2023.pdf.

[19] J. Dahmen, D. J. Cook, X. Wang, and W. Honglei, "Smart secure homes: A survey of smart home technologies that sense, assess, and respond to security threats," *Journal of reliable intelligent environments*, vol. 3, no. 2, p. 1, 2017. DOI: 10.1007/s40860-017-0035-0.

[20] L. Miller, "Integrating smart building predictive maintenance to your system," L. Miller, Ed., accessed: 09.04.2025, Oct. 2024. [Online]. Available: https://web.archive.org/web/20240814031401/https://www.buildingsiot.com/blog/integrating-smart-building-predictive-maintenance-to-your-system-bd.

[21] P. L. Austin, "What will smart homes look like 10 years from now?" accessed: 10.04.2025, Jul. 2019. [Online]. Available: https://time.com/5634791/smart-homes-future/.

[22] X. Guo, Z. Shen, Y. Zhang, and T. Wu, "Review on the application of artificial intelligence in smart homes," *Smart Cities*, vol. 2, no. 3, p. 1, 2019, ISSN: 2624-6511. DOI: 10.3390/smartcities2030025.

[23] L. Budach et al., "The effects of data quality on machine learning performance," 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:251223513.

[24] Y. Chen, "Iot, cloud, big data and ai in interdisciplinary domains," *Simulation Modelling Practice and Theory*, vol. 102, p. 1, 2020, ISSN: 1569-190X. DOI: 10.1016/j.simpat.2020.102070.

[25] Council of the EU, "Data act: Council adopts new law on fair access to and use of data," accessed: 10.04.2025, Oct. 2024. [Online]. Available: https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/contact-tracing-and-warning-apps-during-covid-19_de.

[26] R. K. Institute, "Digitally interrupt chains of infection with the corona-warn-app," accessed: 11.04.2025, May 2024. [Online]. Available: https://www.rki.de/DE/Themen/Infektionskrankheiten/Infektionskrankheiten-A-Z/C/COVID-19-Pandemie/CoronaWarnApp/Warn_App.html.

[27] D. P. Conference, "Use of digital contact tracing services for event, facility, restaurant and business visits to prevent the spread of covid-19: Guidance from the conference of independent federal and state data protection supervisory authorities," Apr. 2021.

[28] EU Commission - Representation in Germany, "Fair digital markets: Gatekeepers must comply with all dma rules starting today," accessed: 10.04.2025, Mar. 2024. [Online]. Available: https://germany.representation.ec.europa.eu/news/faire-digitale-markte-torwachter-mussen-ab-heute-alle-dma-regeln-einhalten-2024-03-07_de.

[29] European Commission, "Communication from the commission to the european parliament and the council: Second report on the application of the general data protection regulation (gdpr)," accessed: 10.04.2025, Jul. 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52024DC0357.

[30] European Parliament and Council of the EU, "Regulation (eu) 2022/1925 of the european parliament and of the council," of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *Official Journal of the European Union*, Dec. 2023, accessed: 09.04.2025.

[31] Deloitte, "Consumer IoT fact check: The internet of things in the everyday lives of german consumers," accessed: 09.04.2025, 2021. [Online]. Available: https://web.archive.org/web/20231214185700/https://www.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Consumer_IoT_2021_Deloitte.pdf.

[32] B. K. Sovacool, D. D. Furszyfer Del Rio, "Smart home technologies in europe: A critical review of concepts, benefits, risks and policies," accessed: 10.04.2025, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032119308688.

[33] European Commission, "Data act – questions and answers," Jun. 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

[34] European Commission, "European data strategy," accessed: 10.04.2025, Nov. 2024. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[35] EU Commission - Representation in Germany, "General data protection regulation: EU commission wants to improve enforcement," accessed: 10.04.2025, Jul. 2023. [Online]. Available: https://germany.representation.ec.europa.eu/news/datenschutzgrundverordnung-eu-kommission-will-durchsetzung-verbessern-2023-07-04_de.

[36] T. Heino, S. Rauti, and R. Carlsson, "An assessment of privacy policies for smart home devices," in *Proceedings of the 24th International Conference on Computer Systems and Technologies (CompSysTech '23)*, T. Vassilev and R. Trifonov, Eds., ser. ACM Other conferences, New York, NY, United States: Association for Computing Machinery, 2023, p. 1, ISBN: 979-8-4007-0047-7. DOI: 10.1145/3606305.3606332.

[37] R. Herold, "Five common privacy problems in an era of smart devices," accessed: 10.04.2025, Jan. 2020. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/five-common-privacy-problems-in-an-era-of-smart-devices.

[38] L. Schoenherr, M. Golla, T. Eisenhofer, J. Wiele, D. Kolossa, and T. Holz, "Unacceptable, where is my privacy?" accessed: 09.04.2025, Nov. 2021. [Online]. Available: https://unacceptable-privacy.github.io/index.html.

[39] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *Internet of Things WF-IoT*, 2014. DOI: 10.1109/WF-IoT.2014.6803194.

[40] N. Olsen, "Voice assistants and privacy issues - privacy policies," N. Olsen, Ed., accessed: 10.04.2025, Jun. 2022. [Online]. Available: https://www.privacypolicies.com/blog/voice-assistants-privacy-issues/.

[41] Consumer advice center, “Smart home - the intelligent home,” accessed: 10.04.2025, Oct. 2024. [Online]. Available: https://www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882.

[42] Federal Office for Information Security, “Identity theft via data leaks and doxing. ”[Online]. Available: https://www.bsi.bund.de/dok/6692610.

[43] J. Thorpe-Smith, “Data Leaks: The Biggest Risks, Consequences, Causes & How to Prevent Them | Metomic,” Nov. 2024. [Online]. Available: https://www.metomic.io/resource-centre/what-are-the-biggest-risks-of-data-leaks.

[44] dpa Service, “Securely networked?: How data protection works in the smart home,” accessed: 10.04.2025, May 2021. [Online]. Available: https://www.zeit.de/news/2021-05/20/so-geht-datenschutz-im-smarthome.

[45] T. J. Heydn, “Advice on drafting contracts for the internet of things (iot),” accessed: 10.04.2025, 2021. [Online]. Available: https://www.tcilaw.de/hinweise-zur-vertragsgestaltung-beim-internet-of-things-iot/.

[46] Consumer advice center NRW, “Data disclosure: How to find out what companies know about you,” accessed: 10.04.2025, 2023. [Online]. Available: https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/datenauskunft-so-erfahren-sie-was-unternehmen-ueber-sie-wissen-44238.

[47] Amazon.de, “Amazon.de privacy notice,” accessed: 10.04.2025, 2024. [Online]. Available: https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=GX7NJQ4ZB8MHFRNJ&language=en_GB.

[48] Amazon.de, “Alexa terms of use,” accessed: 10.04.2025, 2023. [Online]. Available: https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740.

[49] “What is AWS Database Migration Service? - AWS Database Migration Service,” accessed: 09.04.2025, 2024. [Online]. Available: https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html.

[50] European Commission, “Right to repair: Questions & answers,” accessed: 10.04.2025, 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_1795/QANDA_23_1795_EN.pdf.

[51] Q. Baterna, “6 ways to make it harder for data brokers to collect your data,” accessed: 10.04.2025, Nov. 2021. [Online]. Available: https://www.makeuseof.com/ways-to-make-it-harder-for-data-brokers-collect-your-data/.

[52] Federal Ministry for Digital and Transport, “EU verabschiedet data act,” accessed: 10.04.2025, 2023. [Online]. Available: https://web.archive.org/web/20250323125138/https://bmdv.bund.de/DE/Themen/Digitales/Digitale-Gesellschaft/EU-Data-Act/eu-data-act.html.

[53] European Commission, “Frequently asked questions - data act,” accessed: 10.04.2025, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act.

[54] D. Pauly and A. Lohbeck, “Eu: Data act – how fair is the draft regulation for more fairness in the data economy?” accessed: 10.04.2025, 2022. [Online]. Available: https://linklaters.de/insights/publikationen/tmt/datenschutz/2022/februar/eu-data-act.

[55] W. Kerber, “The EU "data act": A critical analysis,” accessed: 10.04.2025, 2022. [Online]. Available: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/prof-wolfgang-kerber/presentation/2022_03_21-kerber-pres-data-act.pdf.

[56] European Data Protection Supervisor, “History of the development of the gdpr,” accessed: 10.04.2025, Dec. 2024. [Online]. Available: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de.

[57] Stiftung Datenschutz (Foundation for Data Protection), BDV e.V., and DIHK, “Data act and gdpr: For more legal clarity on data access and use,” accessed: 10.04.2025, 2022. [Online]. Available: https://dsgvo-2024.org/wp-content/uploads/2022/08/BvD_Stiftung-Datenschutz_DIHK_Positionspapier_Data-Act-und-DSGVO_v1.pdf.

[58] M. Goetz and B. P. Paal, “Between data use and data protection: The relationship between the gdpr, data act and data governance act,” Dec. 2024. [Online]. Available: https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/zwischen-datennutzung-und-datenschutz-438.

[59] S. Piasecki, “Expert perspectives on gdpr compliance in the context of smart homes and vulnerable persons,” *Information & Communications Technology Law*, vol. 32, no. 3, pp. 385–417, 2023, ISSN: 1360-0834. DOI: 10.1080/13600834.2023.2231326.

[60] Harvard Business School Online, “Data analytics privacy issues & how to avoid them,” accessed: 10.04.2025, 2015. [Online]. Available: https://online.hbs.edu/blog/post/data-privacy-issues.

[61] K. Ahuja and M. Patel, “There’s no place like a connected home: Perspectives on the connected consumer in a world of smart devices,” accessed: 10.04.2025, Nov. 2020. [Online]. Available: https://www.mckinsey.com/spContent/connected_homes/index.html.

[62] J. Bugeja, A. Jacobsson, and P. Davidsson, “An empirical analysis of smart connected home data,” in *Internet of Things - ICIOT 2018*, D. Georgakopoulos and L.-J. Zhang, Eds., ser. Information Systems and Applications, incl. Internet/Web, and HCI, Cham: Springer International Publishing and Imprint: Springer, 2018, pp. 134–149, ISBN: 978-3-319-94370-1. DOI: 10.1007/978-3-319-94370-1_10.

[63] D. Bastos, F. Giubilo, M. Shackleton, and F. El-Moussa, “Gdpr privacy implications for the internet of things,” 2018. [Online]. Available: https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things.

[64] V. Dahl and M. Österlin, *Impact of gdpr on data sharing behavior of smart home users*, Oct. 2020.

Strategies for Successful Technology Adoption

Insights from Real-World Implementation Projects

Lasse Berntzen
School of Business
University of South-Eastern Norway
Horten, Norway
e-mail: lasse.berntzen@usn.no

Marius Rohde Johannessen
School of Business
University of South-Eastern Norway
Horten, Norway
e-mail: marius.johannessen@usn.no

***Abstract*—This paper investigates strategies for promoting successful user adoption of new technologies by combining theoretical insights with practical experiences from European research projects. It emphasizes three key enablers: co-creation, content marketing, and trust. Co-creation is highlighted to ensure that systems are aligned with user needs and to foster psychological ownership through early and continuous involvement. Marketing is presented as essential for raising awareness, communicating value, and supporting adoption across different user segments. The paper also examines trust as a prerequisite for adoption, particularly in contexts involving the sharing of data or relinquishing control. A range of established models and theories, including the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT2), Theory of Planned Behavior (TPB), and Diffusion Of Innovations (DOI), are reviewed to provide a foundation for understanding adoption dynamics. The findings suggest that combining theoretical frameworks with user-centered design and effective communication strategies can significantly enhance the adoption of emerging technologies. These insights provide a practical foundation for designing more user-centered, trustworthy, and widely adopted technologies.**

Keywords-technology adoption; co-creation; marketing; trust.

I. INTRODUCTION

Technology adoption refers to the process through which individuals, organizations, or entire societies begin to use and integrate new technologies into their daily lives, work, or operations. It is not just about acquiring new technology but about incorporating it into everyday practice in a meaningful way.

Technology adoption is a multifaceted process influenced by psychological, contextual, social, and communicative factors. This paper presents a theoretical and practical exploration of technology adoption mechanisms, drawing on insights from three diverse projects: Smart-MLA, PVADIP-C, and OptFor-EU.

Smart-MLA [1] was a European project that focused on aggregating and trading energy flexibility in the electricity market. The authors were responsible for identifying potential obstacles to users adopting the Smart-MLA solution and found a lack of trust to be a significant obstacle [2]. The project had partners from Denmark, Norway, Romania, Sweden, and Turkey.

PVADIP-C [3], another European project involving partners from Norway, Romania, and Turkey, has developed a data collection unit and a cloud-based platform that analyzes and diagnoses data from residential or small commercial PhotoVoltaic (PV) installations. The goal was to help prosumers optimize their energy production, improve system efficiency, and maximize financial returns. Here, the focus was on the product itself. What is needed for users to adopt the unit and the platform? In this project, our task was to provide input to the development team on traditional adoption and innovation theories.

The final, and still ongoing, project, OptFor-EU [4], is developing a Decision Support System (DSS) for sustainable forest management. The project involves sixteen partners and eight case studies from different countries. This system is co-created with forest managers and stakeholders to provide tailored, science-based options for climate adaptation and mitigation, focusing on improving Forest Ecosystem Services (FES), including decarbonization and resilience. In this project, we draw on experiences from former co-creation initiatives, complemented by insights into traditional adoption and innovation theories.

In all three projects, a fundamental prerequisite for adoption is user awareness, enabled through effective marketing. Before considering adoption, the user needs to be informed about the product or service.

By synthesizing findings and theoretical frameworks, the paper aims to guide the increase in user adoption of emerging systems.

The rest of this paper is organized as follows. Section II emphasizes co-creation. Section III describes models and theories addressing technology adoption. Section IV addresses marketing and technology adoption. Section V discusses trust and its impact on adoption. Finally, Section VI concludes the paper and provides ideas for future work.

II. CO-CREATION

A key insight from these projects is the value of involving users throughout the design and implementation process. Co-creation [5][6], where users collaborate with developers and designers to define, shape, and test technology, ensures that solutions align with actual user needs and expectations. It also

helps identify usability issues and barriers to adoption early on. Through co-creation, users will not only support development but will also have more substantial ownership of the product.

Tudose et al. [7] have developed a co-creation framework consisting of three iterative stages: co-design, co-production, and co-dissemination, thereby engaging users throughout the lifecycle of the service or product. This framework is embedded in all project activities in OptFor-EU.

Heidenreich, Jordanow, Kraemer, and Obschonka [8] provide theoretical and empirical evidence that:

- User co-creation increases initial adoption: The willingness to co-create significantly shapes usage intention during the pre-adoption stage.
- User co-creation drives continuous engagement: The level of co-creation becomes a significant factor in sustaining long-term usage after the adoption stage.
- Matching user needs is essential: The paper highlights the importance of a "co-creation sweet spot"—the balance between what users are willing to contribute and the degree of co-creation expected. Too high expectations about user involvement may have an adverse effect on willingness to co-create.
- Co-creation fosters psychological ownership: By involving users early, they become more invested in the solution, which enhances satisfaction and commitment, directly supporting your assertion that co-creation leads to a stronger sense of ownership.

In OptFor-EU, for instance, co-design activities in stakeholder workshops helped shape the visual interface and functionality of a forest management decision support system. This participatory approach promotes trust and acceptance. Co-creation aligns closely with service-dominant logic [9] and design thinking methodologies [10], emphasizing iterative development based on continuous feedback. Furthermore, the project employed the co-creation framework to identify and categorize stakeholders, determine how different stakeholders would be engaged, and identify the most suitable engagement methods. It also identified user needs and evaluated the usability of the OptFor-EU forest management DSS. Co-creation activities throughout the project help with technology adoption once the system is ready for implementation [7][11].

III. Technology Adoption

Understanding what drives or hinders the adoption of technology requires a strong theoretical foundation. We present several models and theories that highlight key factors developers should consider when building new systems. An overview of models and theories, along with their relationships, is presented in Figure 1.

Based on the models and theories presented in the OptFor-EU deliverable D5.1 [11], this paper reviews these frameworks. The adoption theories presented in subsections A-C build upon each other to form the UTAUT model, which is then discussed in subsection D. UTAUT serves as the basis for evaluating the systems developed in all three projects. Furthermore, innovation and resistance theories were applied to supplement the co-creation framework in OptFor-EU, addressing specific challenges related to the adoption of technological innovation. Affordance theory also informed stakeholder workshops related to the development of the DSS in the OptFor-EU project.

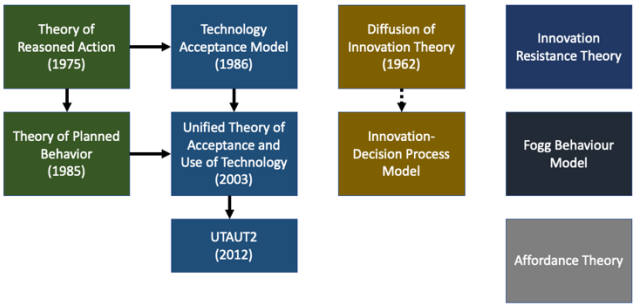

Figure 1. Theories and Models.

A. Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA), developed by Fishbein and Ajzen [12], is a psychological model that explains how intentions and social influences shape human behavior. According to TRA, a person's intention to perform a behavior is the best predictor of whether they will actually do it (see Figure 2). This intention depends on two main factors: the person's attitude toward the behavior and the subjective norms surrounding it.

Attitude refers to how positively or negatively someone evaluates the behavior. This evaluation is based on what they believe will happen if they perform the behavior and how much they value those outcomes.

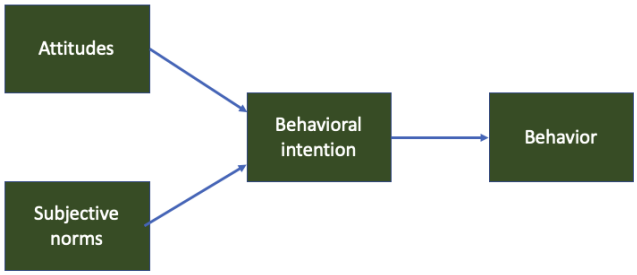

Figure 2. Theory of Reasoned Action (TRA).

Subjective norms relate to perceived social pressure. They reflect what a person thinks is important that others, like friends, family, or coworkers, expect them to do, and how motivated they are to meet those expectations [13].

TRA has been widely applied in areas like health, marketing, and technology adoption. While it does not consider all factors, such as experience or perceived control, it offers valuable insights into how attitudes and social influence shape decisions. This makes it helpful in designing communication strategies and interventions that encourage desired behaviors in specific groups.

B. *Theory of Planned Behavior (TPB)*

The Theory of Planned Behavior (TPB), developed by Ajzen [14], builds on the TRA to better explain behavior in situations where people may not have complete control over their actions.

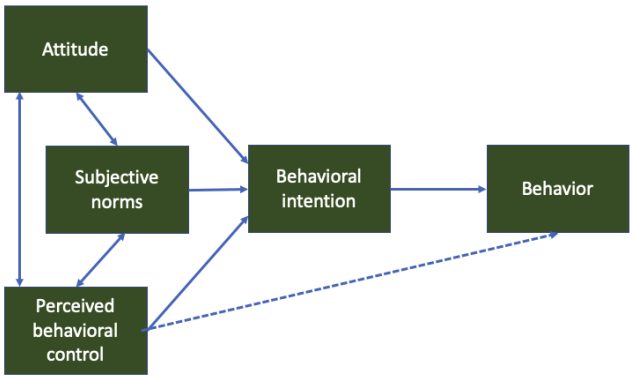

Figure 3. Theory of Planned Behavior.

TPB adds a third key factor to the original model, as shown in Figure 3, perceived behavioral control, which refers to the extent to which people feel they have control over their behavior.

According to TPB, a person's intention to perform a behavior is influenced by three components:

- Attitudes – how positively or negatively they view the behavior, based on what they believe will happen and how much they value those outcomes.
- Subjective norms – the social pressure they feel, shaped by what they think important others expect of them, and their willingness to meet those expectations.
- Perceived behavioral control – how easy or difficult they think it will be to carry out the behavior. This includes both internal factors (such as skills and confidence) and external ones (such as time, resources, or support).

TPB has been applied in various areas, including health, environmental actions, and technology adoption [15]. By considering the extent to which people feel they have control, TPB offers a more realistic view of behavior. It helps researchers and practitioners design strategies that better align with individuals' abilities and the challenges they encounter in various settings.

C. *Technology Acceptance Model (TAM)*

The Technology Acceptance Model (TAM), created by Davis [16], is one of the most widely used models for understanding why people accept or reject new technologies. It was developed as an extension of the TRA, with a specific focus on the use of technology.

TAM proposes that a person's intention to use a technology is mainly influenced by two factors: perceived usefulness and perceived ease of use (see Figure 4).

- Perceived usefulness refers to the extent to which a person believes the technology will enhance their performance or aid them in achieving their goals.
- Perceived ease of use refers to how effortless users think it will be to use the technology.

These perceptions shape the person's attitude toward using the technology, which then affects their intention to use it. This intention is considered a strong predictor of whether they will actually use the technology.

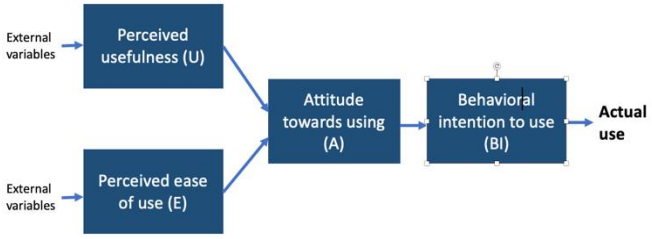

Figure 4. Technology Acceptance Model (TAM).

Over time, TAM has been expanded to include other relevant factors, such as social influence (subjective norms), perceived risk, and trust. Despite being a relatively simple model, the Technology Acceptance Model (TAM) has proven to be a robust and reliable framework across various technologies and user groups. It remains a valuable resource for both researchers and practitioners aiming to promote effective technology adoption.

D. *Unified Theory of Acceptance and Use of Technology (UTAUT and UTAUT2)*

The Unified Theory of Acceptance and Use of Technology (UTAUT), developed by Venkatesh and colleagues [17], brings together elements from eight different technology adoption models, including TRA, TAM, and TPB, and is the result of more than three decades of research on user adoption. Its goal is to offer a broader and more complete view of what influences people to adopt new technologies.

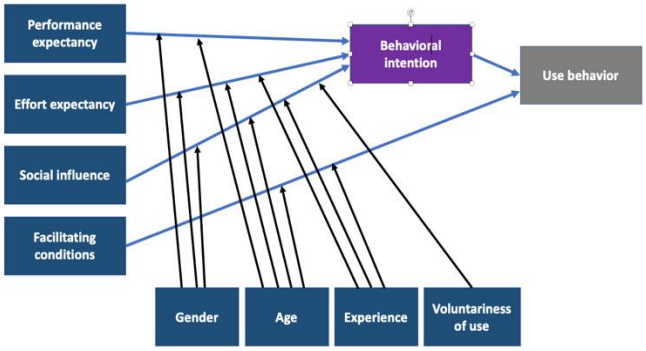

Figure 5. UTAUT.

As shown in Figure 5, UTAUT identifies four main factors that drive technology acceptance and use:

- Performance expectancy: the belief that using the technology will lead to better performance or help achieve meaningful goals.
- Effort expectancy: the belief that the technology will be easy to use.

- Social influence: the perception that people around you think you should use the technology.
- Facilitating conditions refer to the availability of support, training, or resources that enable the use of technology.

The model also considers that individual differences, such as gender, age, experience, and whether technology use is voluntary, can affect how these factors influence behavior.

Since its introduction, UTAUT has been widely applied and extensively tested in various areas. It has proven to be a strong framework for understanding and encouraging technology adoption. In 2012, the model was extended (UTAUT2) with three additional factors: hedonic motivation (enjoyment or fun), price value, and habit [18].

E. Diffusion of Innovations Theory (DOI)

The Diffusion of Innovations Theory (DOI), developed by Everett Rogers in 1962 [19], explains how new ideas and technologies spread within a society. It examines why some innovations are rapidly adopted, while others take longer to adopt or fail altogether. Drawing on fields such as sociology, psychology, and communication, the theory identifies key factors that influence adoption.

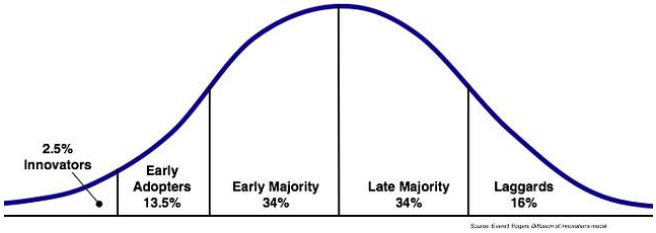

Figure 6. Diffusion of Innovations Theory [19].

According to the DOI, innovations spread gradually through a population as people make decisions to adopt based on five main characteristics:

- Relative advantage – how much better the innovation is compared to what it replaces.
- Compatibility – how well it fits with existing values, needs, or experiences.
- Complexity – how easy or difficult it is to understand and use.
- Trialability – whether it can be tested or tried on a limited basis.
- Observability – how visible the results are to others.

These factors shape how quickly and widely an innovation is adopted. The model also describes the typical user distribution over time, which includes innovators, early adopters, early majority, late majority, and laggards (Figure 6).

F. Innovation-Decision Process Model (IDPM)

The Innovation-Decision Process Model (IDPM), introduced by Everett Rogers as part of the Diffusion of Innovations Theory, outlines five key stages that individuals typically undergo when deciding whether to adopt a new idea or technology [19].

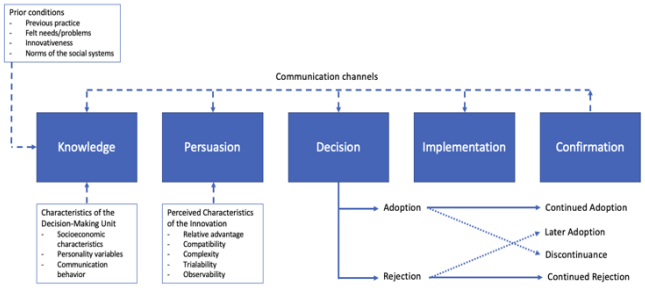

Figure 7. Innovation-Decision Process Model.

These stages, shown in Figure 7, are: knowledge, persuasion, decision, implementation, and confirmation.

- In the knowledge stage, individuals first learn about the innovation and begin to gather information.
- During persuasion, they form an opinion, whether positive or negative, based on how helpful or appealing the innovation appears to be, as well as their past experiences.
- The decision stage is where they choose to adopt or reject the innovation.
- If they adopt it, the implementation stage follows, where the innovation is put into use in real-life situations.
- Finally, in the confirmation stage, individuals look for support or feedback that confirms their decision. If their experience is positive, they continue using it; if not, they may stop.

Understanding these stages enables researchers and practitioners to design more effective strategies and support mechanisms that guide users through the adoption process.

G. Innovation Resistance Theory

Innovation Resistance Theory (IRT) helps explain why people may hesitate or refuse to adopt new ideas, products, or technologies—even when those innovations offer clear benefits [20]. While most adoption theories focus on what encourages people to adopt innovations, IRT examines the obstacles that slow down or block adoption.

Resistance can stem from personal factors, such as habits, preferences, or a fear of change, as well as social and cultural influences, including norms or values that conflict with the innovation.

A key part of IRT is the distinction between two types of resistance:

- Active resistance is a conscious decision to reject an innovation, often because it feels incompatible with one's values, beliefs, or lifestyle.
- Passive resistance is more subtle and may result from a lack of awareness, uncertainty, or difficulty understanding the innovation. In these cases, people tend to stick with what they already know.

For successful innovation adoption, it is important to recognize and address these forms of resistance. This may involve providing better information, offering demonstrations or training, clarifying misconceptions, or gaining support

from trusted influencers. By considering both what encourages and what blocks adoption, IRT provides a more comprehensive picture of how innovations spread [21].

H. Fogg Behavior Model

The Fogg Behavior Model (FBM) [22], created by B.J. Fogg, explains how behavior happens by combining three key elements: motivation, ability, and triggers.

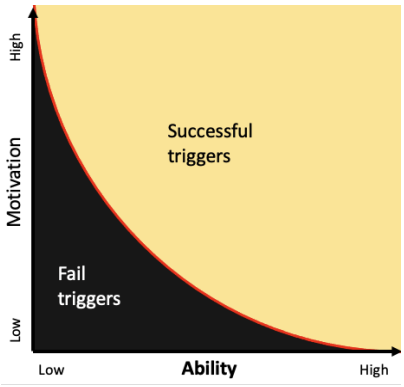

Figure 8. Fogg Behaviour Model.

According to the model shown in Figure 8, a person will only perform a behavior if all three elements come together simultaneously.

- Motivation refers to the degree of desire or enthusiasm someone has for doing something. It can be influenced by factors like pleasure or pain, hope or fear, or the desire for social acceptance.
- Ability refers to how easy or hard it is to do the behavior. If something is too complicated, time-consuming, or expensive, people are less likely to do it, even if they are motivated.
- Triggers (also known as prompts or cues) are signals that prompt the person to take action. This could be a notification, a reminder, or a change in the environment.

If motivation is high and the task is easy, only a small trigger is needed. But if either motivation or ability is low, the behavior is unlikely to happen, even with a strong trigger.

The FBM is especially useful for designing technology, apps, or campaigns that aim to change behavior. By adjusting motivation, enhancing ease of use, or selecting the optimal moments to prompt action, designers can increase the likelihood that users will adopt new behaviors.

I. Affordance Theory

Affordance Theory, first introduced by psychologist James J. Gibson [23], focuses on how people perceive and interact with their environment. An affordance is a feature of an object or system that suggests how it can be used. For example, a button “affords” pushing, and a handle “affords” pulling.

In the context of technology and design, affordances help users understand what actions are possible. If a website or app clearly shows what you can click, swipe, or type into, it is easier and more intuitive to use. These clues can be visible, such as a clickable icon, or hidden, like a keyboard shortcut (see Figure 9), allowing designers to create more user-friendly technologies that feel natural and require less explanation.

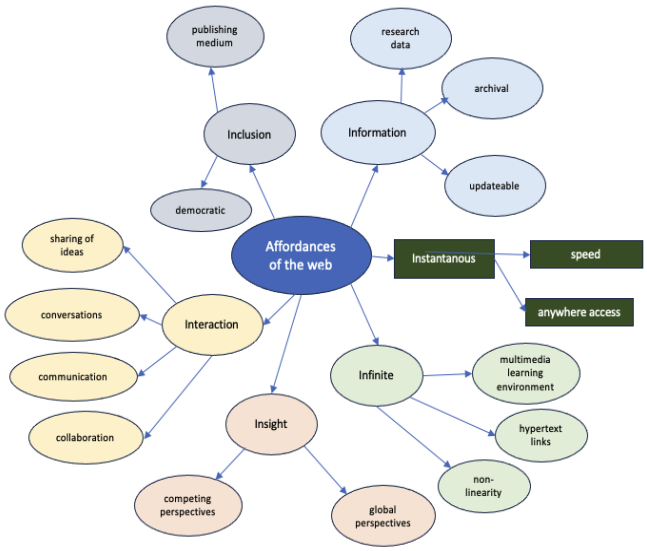

Figure 9. Affordance Theory Example.

The theories presented in this section, summarized in Figure 1, were applied across the three projects. The adoption and diffusion theories enabled us to examine the willingness to adopt smart grid and smart home solutions in Smart-MLA and PVADIC-C. They will be used to analyze the business model and implementation strategy for the OptFor-EU DSS. In contrast, affordance and adoption theories informed the user involvement plan presented in [11] and were applied in stakeholder workshops to elicit user requirements.

IV. Marketing and Technology Adoption

A recurring theme across practical implementations is that technology does not sell itself. Proactive and strategic product or service marketing is essential for bridging the gap between innovation and user readiness. Heiman, Ferguson, and Silberman [24] used agriculture as a field to investigate the relationship between user adoption and marketing. They concluded that this relationship is important for innovations.

We have already emphasized the importance of connecting with users through co-creation; marketing builds on this by ensuring that users understand what is being offered, why it matters, and how it fits their needs. Beyond raising awareness, marketing helps build trust and communicate the value that drives adoption. Effective marketing strategies for technology adoption include:

- Explainer videos and infographics that clarify complex features.
- User testimonials and pilot project stories that build credibility and relatability.
- Scenario-based demonstrations that show how the technology solves real-world problems.

- Targeted messaging that reflects user motivations, such as financial savings, convenience, or sustainability.

Personalized communication and segmentation are essential for reaching diverse user groups, from early adopters who seek technical depth to later adopters who prefer use-case-driven materials.

Marketing should also evolve across the adoption journey, from initial exposure to onboarding and ongoing engagement.

Another key strategy is to maintain a continuous dialogue with users through newsletters, FAQs, and forums. This fosters trust, provides feedback for improvement, and reinforces user commitment. Ultimately, effective marketing is not just about promotion—it is about building understanding, reducing uncertainty, and supporting the journey from awareness to regular use.

Strategic marketing should be viewed as a core part of the adoption process, not an afterthought.

V. Trust and Technology Adoption

Trust is a fundamental prerequisite for the adoption of technology, especially in systems that require users to share data or relinquish control. In previous work [25], we identified three main categories of trust-building measures: regulatory, technical, and organizational.

- Regulatory measures provide stability and predictability through clear rules, certifications, and legal frameworks that reduce uncertainty and define user rights and responsibilities.
- Technical measures focus on system transparency, data security, reliability, and ensuring users have control over their personal information.
- Organizational measures address fairness, accountability, and openness—for example, through user-centered governance and clear, consistent communication.

While not a separate category, the use of plain language across all three domains is vital to ensure users understand how systems work, reinforcing transparency and reducing uncertainty.

Evidence from Smart-MLA showed that users were hesitant to relinquish control over their home energy use to aggregators, even when financial incentives were offered—unless they trusted the system and its operators [2]. This highlights the importance of both technical safeguards and effective communication.

In public sector contexts, partnering with trusted institutions can further increase confidence. Users are more likely to adopt a technology when they believe it operates fairly and in their best interest.

In today's environment, shaped by misinformation and the growing presence of generative AI, building and maintaining trust is more challenging than ever. To do so, three actions are essential:

- Transparency – Clearly explain how the system works, what data is collected, and how it is used.
- Reliability – Ensure the technology performs consistently and is backed by responsive support.
- Social proof – Use testimonials, endorsements, and visible success stories to show that others trust and benefit from the solution.

Together, these elements form the foundation for user trust, an essential driver of successful and sustained technology adoption.

VI. Conclusion and Future Work

Successful technology adoption is not solely driven by technical merit; it relies on a combination of human-centered strategies and foundational theoretical understanding. This paper has highlighted three essential enablers of adoption: co-creation, marketing, and trust. Co-creation ensures that technologies are aligned with user needs, promoting long-term engagement by fostering ownership and relevance. Marketing bridges the gap between innovation and awareness, providing tailored communication that resonates with user motivations and informs decision-making. Trust, as demonstrated through regulatory clarity, technical reliability, and transparent organizational practices, is a prerequisite for acceptance, particularly in systems that involve data sharing or automated control.

By combining these practical strategies with well-established models such as TAM, UTAUT2, TPB, and DOI, we gain a robust foundation for designing, promoting, and implementing user-centered technologies. We have briefly mentioned how our three projects have applied these strategies and theories in this paper; however, due to space constraints, we refer readers to the project websites for more detailed information. Future technology initiatives—whether in public or private sectors—will benefit from viewing adoption not as a final step, but as a continuous process rooted in mutual understanding, clear communication, and sustained trust.

In this paper, we demonstrate how to combine practical and theoretical frameworks to increase the chances of successful technology adoption. By following a co-creation approach throughout the project, we ensure that stakeholders and users are involved in everything, from gathering requirements and defining functionality to front-end design and the usability of the system. By utilizing adoption theories (subsections III.A-D), we have both a framework for evaluation and theoretically sound input to what should be emphasized in the co-creation process, especially if affordances (section III.I) are part of the co-creation process regarding requirements and functionality. Innovation theories inform us on how to transition from a research project to implementation. They should, therefore, be integrated into business models to realize the value of software-based research projects, along with the marketing components outlined in Section IV.

Finally, we emphasize the role of trust in Section V. This is not something that a project group can fully control, as it requires regulatory measures and a general level of trust in society. Still, project organizations can implement policies that facilitate trust among project members, while also aiming

for transparency, reliability, and social proof of the software solution.

ACKNOWLEDGMENT

This work was partially funded by the European Union Horizon Europe program, under Grant agreement n°101060554.

Co-funded by the European Union

Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union or REA. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] Smart-MLA, Project website, [Online]. Available from: https://smart-mla.stimasoft.com 2025.04.01

[2] M. R. Johannessen et al., "User Sentiments Towards Smart Grid Flexibility - A survey of early adopters' attitude towards allowing third parties to control electricity use in households," Proc. 14th International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC), pp 41-46, 2021.

[3] PVADIP-C, Project website [Online]. Available from: https://www.icpe.ro/pvadipc/ 2025.04.01

[4] OptFor-EU, Project website. [Online]. Available from: https://optforeu.eu/partners/ 2025.04.01

[5] V. Ramaswamy and F. Gouillart, The Power of Co-Creation, Free Press, 2010.

[6] V. Ramaswamy and K. Ozcan, The Co-Creation Paradigm, Stanford University Press, 2014.

[7] N. C. Tudose et al., "Challenges and opportunities of knowledge co-creation for the water-energy-land nexus," Clim. Serv. 30. 2023.

[8] S. Heidenreich, S. Jordanow, T. Kraemer, and M. Obschonka, "Together Forever? How customer co-creation affects the adoption of digital service innovation over time," Journal of Product Innovation Management, 41 pp. 1062–1090, 2024.

[9] S. L. Vargo and R. F. Lusch, "Service-dominant logic 2025," International Journal of Research in Marketing, 34(1), pp. 46-67, 2017.

[10] T. Brown, "Design Thinking," Harvard Business Review, 86(6), pp. 84-92, 2008.

[11] L. Berntzen and M.R. Johannessen, User Adoption. – Customization and user involvement strategy. OptFor-EU deliverable 5.2. [Online]. Available from: https://optforeu.eu/wp-content/uploads/2024/01/OptFor-EU_D5_1_user-adoption-2nd-revision.pdf 2025.04.01

[12] M. Fishbein and I. Ajzen, Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley, 1975.

[13] I. Ajzen and M. Fishbein, Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall, 1980.

[14] I. Ajzen, "The theory of planned behavior," Organizational Behavior and Human Decision Processes, 50(2), pp. 179-211, 1991.

[15] I. Ajzen, "The theory of planned behaviour: Reactions and reflections," Psychology & Health, 26(9), pp. 1113-1127, 2011.

[16] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly 13(3), pp. 319-340, 1989.

[17] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly 27 (3), pp. 425-478, 2003.

[18] V. Venkatesh, J. Y. L. Thong, and X. Xu, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," MIS Quarterly 36(1), pp. 157-178, 2012.

[19] E. M. Rogers, Diffusion of Innovations. 5th ed. Riverside: Free Press, 2003.

[20] J. N. Sheth, "Why we buy what we buy: A theory of consumption values," Journal of Business Research, 9(2), pp. 159-170, 1981.

[21] S. Ram and J. N. Sheth, "Consumer Resistance to Innovations: The Marketing Problem and its solutions," Journal of Consumer Marketing 6(2), pp. 5–14, 1989.

[22] B. J. Fogg, "A behavior model for persuasive design," In: Samir Chatterjee (Hg.): Proceedings of the 4th International Conference on Persuasive Technology. Claremont, California, USA. Association for Computing Machinery. New York: ACM, pp. 1–7, 2009.

[23] J. J. Gibson, The ecological approach to visual perception. Hillsdale, N.J.: Erlbaum, 1986.

[24] A. Heiman, J. Ferguson, and D. Silberman, "Marketing and Technology Adoption and Diffusion," Applied Economic Perspectives and Policy, 42(1), pp. 21-30, 2020.

[25] L. Berntzen, M. R. Johannessen, and Q. Meng. "The Aggregator as a Trust Builder in a Renewable Energy System," 17th International Conference on Digital Society (ICDS), pp. 63-68, 2023.