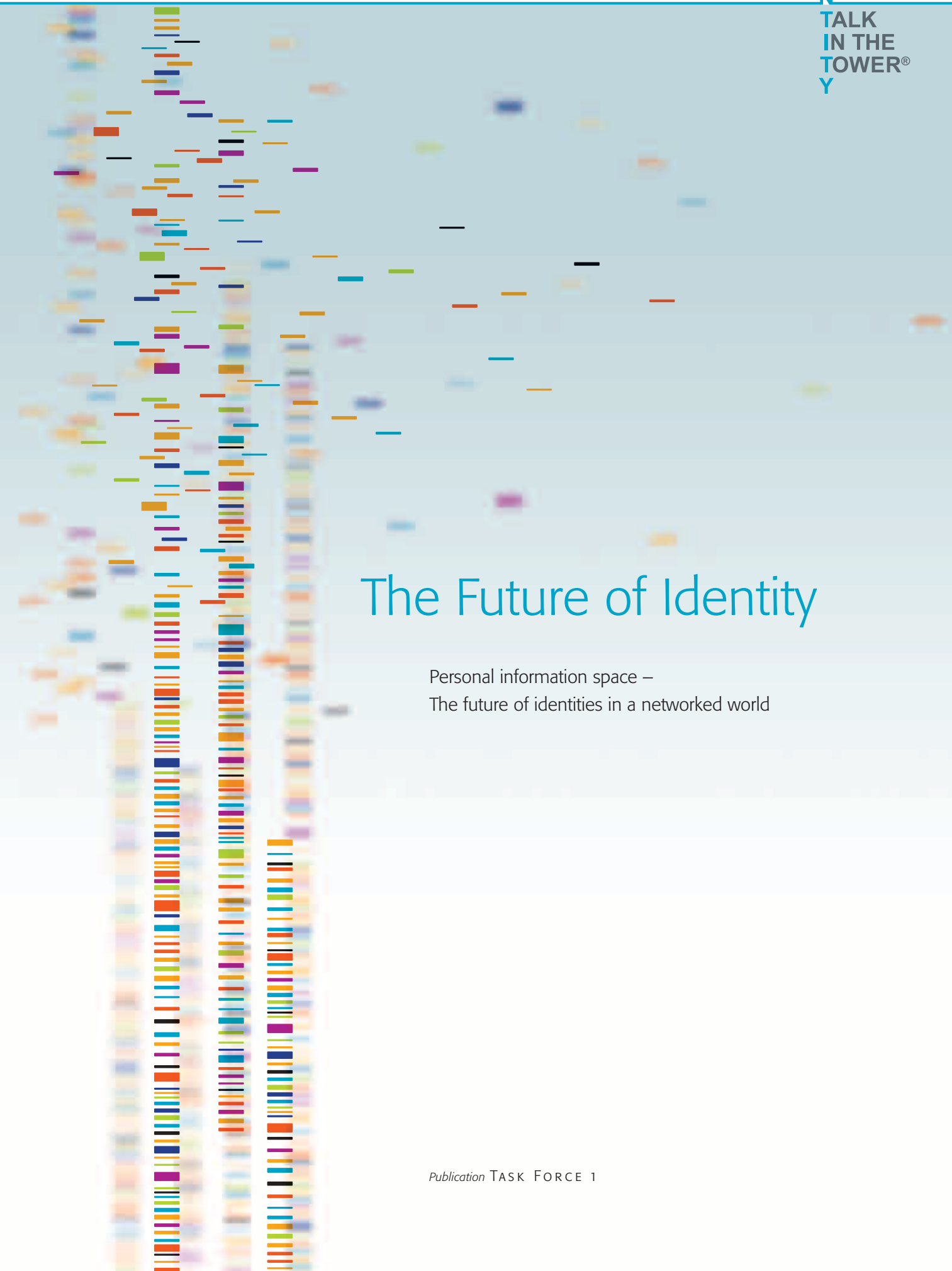
IDENTITY TALK IN THE TOWER®



The Future of Identity

Personal information space –
The future of identities in a networked world

Publication TASK FORCE 1

TABLE OF CONTENTS

PREFACE

Identity – Talk in the Tower

IDENTITY – Talk in the Tower®[1] is the platform for open, ongoing, and cross-border discussion on the future of identity in our fast-changing digital age. By bringing together a wide range of experts – academic, commercial, and technical – the platform is helping to stimulate an inter-disciplinary exchange of out-of-the-box ideas about what is happening to our identities, now and in the future.

In working groups known as Tower Task Forces, these expert participants investigate in greater detail topics and issues previously identified by respected leaders and thinkers in so-called Tower Talks. This report represents the work of one such Task Force, which has examined the Role of Machines.

Giesecke & Devrient's Engagement

As suppliers of end-to-end security solutions for both businesses and governments, identity and its protection are at the core of our business. Indeed, thanks to the technologies we produce, we are on the leading edge of the transformation that is driving interest in identity.

Founded more than 160 years ago as a producer of banknotes, G&D now also supplies travel documents, ID systems, and health-care cards to governments worldwide, as well as providing banks, mobile network operators, original equipment manufacturers, and others with mobile security applications, especially for telecommunications and electronic payments.

These systems, by definition, need to be secure. Which is why trust, security, and competence have been our watchwords ever since our foundation. We are also committed to taking responsibility for our actions and their impact on society. We believe that responsibility requires dialog; that dialog, indeed, inspires confidence – hence our IDENTITY – Talk in the Tower initiative.

Overview of Participants

The Task Force participants represent a broad range of professional interests — from lawyers and philosophers to IT and communications specialists. In order to ensure a truly international perspective, we also applied regional criteria to their selection, though Europeans predominate. Each Task Force participant is an expert in his or her particular field. For detailed profiles, please see page 23.

EXECUTIVE SUMMARY

This report explores the role of machines in our concepts of identity. In the view of the Task Force, machines act as the technological mediator between the individual end user and their "personal

[1] *For further information, please visit our website www.identity-tower.com*

information space," which is defined as the sum of our personal data. In order to understand better the implications of the impact of machines on our future identities, in the sense of personal information spaces, the Task Force conducted a scenario workshop, designed to show which evolving forces are most likely to influence our daily life and what this could mean for our personal information space within the European Union ten years from now – in 2023.

The scenarios do not claim to be inclusive. Nor do they cover every nuance of the developments under consideration (though the remarks of four expert commentators do suggest some additional aspects for consideration). It is hoped, however, that they present a realistic view of future possibilities.

Two scenarios are addressed: one concerned with a situation of distributed power; and the other with a situation where a single provider exercises centralized control. It seems likely that a mixture of both is the most likely future outcome. But we hope that the ideas presented will provoke further thought about related (and much more complex) questions.

INTRODUCTION

Identity and the Role of Machines

Established after the first Tower Talk discussion, which took place in Berlin, Germany, in May 2012, Task Force 1 has focused on the role of machines in our changing concepts of identity.

Why "machines," rather than "technology," which is, after all, a more contemporary notion? Because technology is just one of the multitude of non-human forces — robots, devices, tools, infrastructure, connectivity, the digital environment, the Internet, the "Internet of Things," software, algorithms, platforms — that are impacting our concept of identity.

There may not even be one single word to describe these forces; but in the view of the Task Force, machines, as a generic construct, provides an appropriate descriptor for the purposes of their study.

The Task Force, indeed, sees machines as the technological mediator between the individual end user and the information space, which today can be defined as the "personal information space" — or identity as the sum of our personal data *(see **Fig. 1**)*.

Our identities, in the sense of personal information spaces, change according to the various environments in which we act – business, cultural, administrative, or legal. However, while in the past it was relatively easy to distinguish these different identities from each other, today, thanks to the collective impact of the forces described above, it has become much more difficult.

In an effort to deconstruct some of this complexity, and to understand better the implications of the impact of machines on our future identities, the Task Force conducted a scenario workshop.

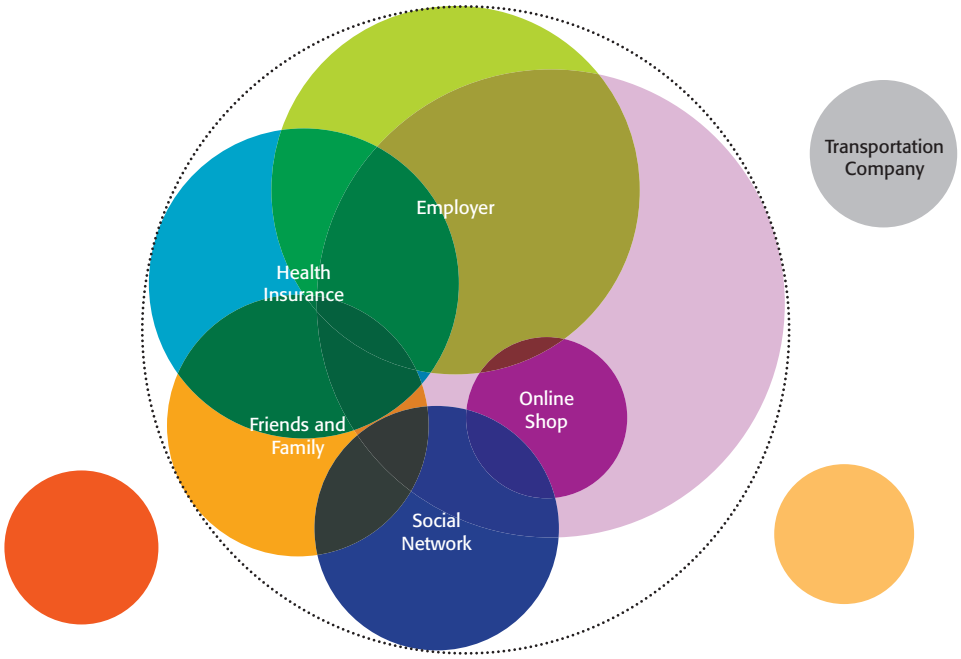


Fig. 1
***Personal Information Space in 2013** –*
Third-party access to personal data

The Scenario Approach

Scenarios are stories about how the future might unfold. They are not predictions, but rather provocative and plausible accounts of how relevant external forces (in this case, machines) might interact and evolve to influence our environment (in this case, our personal information space). The purpose of scenario thinking is not to identify the most likely future but to create a map of uncertainty – capturing a range of possibilities, good and bad, expected and surprising.

Rather than try to reveal how the interaction with machines will change our identity, the Task Force used the scenario approach to show which developing forces will likely influence our daily life and what this could mean for our personal information space.

The reader should note, however, the limitations of the scenarios. They provide only snapshots of possible future developments, not exhaustive accounts. Nor do they claim to include all possible nuances of the developments under consideration (though some additional aspects are suggested by our four expert commentators; see page 15 to page 20). The scenario protagonists, moreover, are largely passive participants in their environments; they do not offer criticisms of these environments, but only describe the evolving impacts on their daily lives. We believe,

nonetheless, that this attempt to foresee the evolution of identity distinguishes the work of the Task Force from other scenario work in this field, which tends to focus on the evolution of future technologies.

To focus its approach, the Task Force chose to imagine a future ten years from now – 2023 – and geographically limited to the European Union. In order to widen its perspective, two alternative scenarios were chosen: one concerned with a situation where a single provider exercises centralized control; and the other with a situation of distributed power.

The Task Force participants' principal concern was to take as realistic a view of the future as possible. The reader will not find a "sci-fi" world under discussion, but will recognize many services and features – apps, for instance – that exist today (and may well continue to exist in 2023). By dealing with the familiar, it is hoped that the activities of the two scenario protagonists, Anna and David, will be easier to grasp for people interested in the topic, but without deeper expert knowledge.

HOW WILL THE PERSONAL INFORMATION SPACE LOOK TEN YEARS FROM NOW IN THE EUROPEAN UNION?

Scenario One

Profile:
David, male, 48 years old, European, works for the government in communications, is – like his father – a big Rolling Stones fan, has his own blog "David's Drum Diaries."

November 28, 2023. I must have overslept! Skipping my usual routine of skimming through news streams and social networks for twenty minutes, I quickly shower and get dressed before rushing out the door. I jump into one of the automatic electric cars to get from the outskirts to town. Even though I generally prefer being the driver myself, I've always been curious about the automatic cars. And since they introduced them to my town, I've come to really enjoy using them. No traffic jams, hardly any accidents and you don't have to think about whether dining out after work should or should not include a tasty French wine.

As I like spending the weekends in the countryside there are still plenty of opportunities to test drive my brand new electric sportster. And using the automatic cars has other advantages. The signage is integrated into the on-windshield display, for example. (They recently removed all signage on the side of the street and replaced it with shrubs.)

The latest news and additional information from local authorities is shown on the display, which is invisibly integrated into the windshield. All relevant information is directly and automatically uploaded into the car, via the Web. Local authorities can alter markers to facilitate smoothly running traffic, avoid jams, and achieve an equal load on the roads. However, the longer the system is

running the less they have to intervene, as the system automatically saves changes, links them to the respective circumstances, and thus learns how to avoid problems in the future. The drive takes no longer than twenty minutes – I still remember the time when traffic overload could mean that a single journey would take up to two hours. This is enough time to get up to date on the news and current events and to check my e-mail. (The latter is on my phone as I still don't really trust the built-in emailing system much; though the mobile Internet installed in all cars renders connectivity issues obsolete.)

I was originally among the critics who opposed opening the windshield display to private advertisements, but they have actually facilitated the introduction of automatic cars. They amortize quickly and the costs for the monthly transport rate can be kept very low. This is calculated by an app in my mobile phone, which automatically connects to the car, enables me to use it, and exchanges data about the duration of the voyage. (I'm not worried about this aspect of automation as only the mileage is recorded and the built-in privacy extensions hinder a linkup to geolocation data.) Besides, the system persuaded me to book tickets for the Rolling Stones® revival concert tomorrow night. I'm already curious to see if Charlie Watts will still be able to play the drums for more than half an hour. When I arrive at the park-and-ride, the car is automatically charged by the induction parking lot. It transfers its remaining energy into the grid to support the early-morning energy requirement peaks. It will be charged again when electricity consumption declines and so will be ready for my ride home.

The ID attached to the car allows the power company to distinguish the car from other electronic devices that can be charged in one of its numerous stations and thus enables the company to credit the power delivered into the system and to debit recharging the car. At the end of the month the public authority that runs the automatic cars will receive a detailed report, and once that report has been accepted, detailed records are erased. What a waste of paper we caused when we still thought that invoices needed to be physically opened and filed away in ring binders. I enter the local rail network. I don't need a subscription. Just passing the sensor at the entrance instantly recognizes me. What's more, there's a Web application in my mobile that knows my daily movements and opens automatically to ask me to confirm that I want to alight at the usual station. Both my presence and my destination are stored in my mobile device.

I love this decentralization of data. It makes me feel in control. I can fill in the information on the train journey. Both my favorite stations and the frequency of my trips are stored in my mobile device. Once a month and once a year, the train company can download the information aggregated by my mobile device that is no longer identifiable — and still forward the respective charge to me, which I can pay immediately. (The app allows me to use a "pay now" button, which in turn is linked to one of my secure payment accounts.) The accuracy of the statistics is continuously improving and helps a great deal with urban planning. No ID is needed. Unfortunately, I can't work while commuting. It's just not safe and my business data is automatically blocked. Well, that's our company policy and they are right to be strict about it. Less cautious companies have lost a lot of data when hackers discovered that the public transportation Wi-Fi provides a back door to access business secrets. I use the time to write a new blog entry instead. But despite my

sympathy for maintaining business secrets, it would be a great time saver if I could do some work here, too. The business partner that I was visiting abroad last week — we went to an overseas conference together — finished his entire presentation while traveling on the metro, while I could only update my personal status and have a quick chat with friends.

David finds out later that the log-in information for his social network provider was stolen while he was abroad and somebody posted in his name on his profile website. The posting was so offensive – including racist statements and inappropriate wording – that his provider blocked his profile altogether. Since the incident happened outside the EU, in a jurisdiction where other regulations apply, David had difficulties proving his innocence. Nevertheless, because he had all his profile information anyway, he could easily change to another social network and stay in touch with his contacts – some of whom didn't even recognize the change.

Blog entry finished. (I'm already curious to read the comments on my "Save your soul, once a month no Wi-Fi in the metro" thesis). Now let's see what my friends are up to … Five years ago, we would have needed to be members of the same social network but now my friends have accepted that I've chosen another, more decentralized network. And in their view, I'm still alive! My friends, like many people, agreed to a standard that determines the unique endpoint of a communication in a social network — very similar to e-mail addresses.

Event streams are transferred between social networks. Some very trendy networks even take money for their event stream because they host all the stars and celebrities; more personal event streams are usually free of charge. The event streams have ID and privacy information that determine access, expiry date, and some other limitations. The reason why I changed to the other network in the first place was that I took up working for the government. When the formerly dominant network provider was sold to an unwanted third party, I decided to pull the ripcord. This third party still knows from open data that I work for the government. And as they have a great interest in influencing future policies I want to make sure that at least they don't know who my family and friends are.

My cousin told me recently that a colleague of his tried to justify his sloppiness about health issues only to discover, ten minutes later, that he was top news on a microblogging service. (It was a quiet day without incidents.) His private health insurer now wants to re-evaluate his rate. But as the message was accidentally published and not sent by him, the insurer had to back off. After all, information use limitations are now also enshrined in law. When he asked the microblog to remove the message they refused and redirected him to an online dispute resolution service where currently an elected board is determining if his privacy has been unduly invaded and thus whether his rights have been infringed. They now have the opportunity to scrutinize the nature of the publication and thankfully have the power to remove the message by issuing a service message into the event stream.

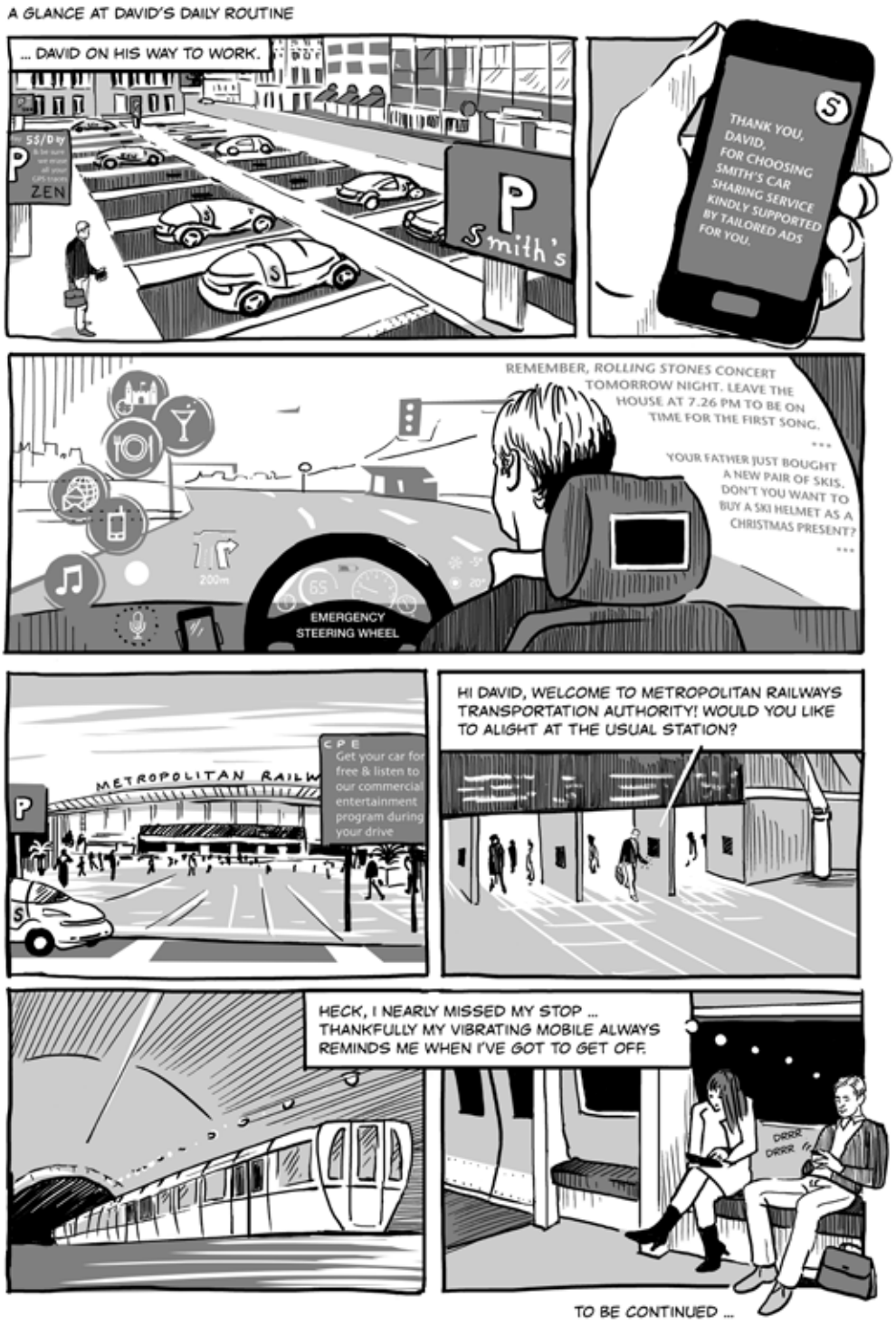
My alarm reminds me that when I get back tonight, I have to remember to buy milk. Unfortunately, my fridge doesn't order it automatically yet. However, it's still fun to go to one of the old-fashioned stores with human cashiers. They always know rumors that nobody has dared to post on the net yet.

Heck, I nearly missed my train station. Thankfully the train reminds me – or rather reminds my mobile, which starts to vibrate. When I get to the office, I wonder why they still haven't replaced the old-fashioned door, which requests an actual swipe of my card, with a device that can read it while it's still in my pocket. Well, I guess while you can't stop technological developments, you can't expect too much at once either.

When I get home in the evening, I attempt to make some progress on my thesis. I'm doing a Master's degree in informatic geography at a distance learning university. We learn how to use hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information. For one of my papers, I'm researching the "happiness index" in relation to eight other social indicators. Some of the data for these indicators are not explicitly available, but with Big Data it's possible to use repositories of social and transactional data, collectively known as the "digital commons." Marketers and others have had access to this kind of data for so long, it made sense for the EU to promote Big Data as a kind of digital commons. Almost any member of the public can use this data now. Municipal library branches offer tutorials on how to search through it. In fact, this training is mandatory for first-year Bachelor degree students.

Purchasing habits, media consumption, and travel plans are all retrievable on these commons. Of course, it's all anonymized. Almost all transactional data is available at a national level, but you have access to less and less data as you increase the resolution, so a postal code search won't yield much (much to the chagrin of stalkers, I'm sure). Coordinating information between municipal, regional, and national governments along with the EU was a bureaucratic nightmare, but not one without precedents! What's more, citizens have a right to opt out of including their data in the commons, though this is a lengthy process. My primary focus is on media consumption habits, although the digital commons don't include media that are streamed illegally on "pirate" sites. I must not forget to acknowledge this as a limitation in my methodology section.

I continue my research for a few hours before retiring to bed. Still a bit restless from my evening coffee, I decide to watch a movie. I have a preferred service for entertainment streams, but my colleagues keep insisting that I try a new, competing service. It's a few euros cheaper per month, plus it somehow has access to a lot of older content that has not been picked up elsewhere. I decide to check out the site, but the registration form is so long! No longer feeling the effects of the caffeine, I go to sleep. This is probably for the best, as I hear that always falling asleep in front of a screen can be harmful to the eyes.


A GLANCE AT DAVID'S DAILY ROUTINE
... DAVID ON HIS WAY TO WORK.
ZEN
Smith's
THANK YOU, DAVID, FOR CHOOSING SMITH'S CAR SHARING SERVICE KINDLY SUPPORTED BY TAILORED ADS FOR YOU.
REMEMBER, ROLLING STONES CONCERT TOMORROW NIGHT. LEAVE THE HOUSE AT 7.26 PM TO BE ON TIME FOR THE FIRST SONG.
YOUR FATHER JUST BOUGHT A NEW PAIR OF SKIS. DON'T YOU WANT TO BUY A SKI HELMET AS A CHRISTMAS PRESENT?
EMERGENCY STEERING WHEEL
METROPOLITAN RAILW
Get your car for free & listen to our commercial entertainment program during your drive
HI DAVID, WELCOME TO METROPOLITAN RAILWAYS TRANSPORTATION AUTHORITY! WOULD YOU LIKE TO ALIGHT AT THE USUAL STATION?
HECK, I NEARLY MISSED MY STOP ... THANKFULLY MY VIBRATING MOBILE ALWAYS REMINDS ME WHEN I'VE GOT TO GET OFF.
DRRR DRRR
TO BE CONTINUED ...

Scenario Two

Profile:
Anna, female, 24 years old, European, junior manager at a logistics company, likes to read, loves Asian food and holidays in France.

November 28, 2023, just another typical day. Though, looking through my window, it looks like a beautiful golden autumn day outside. I finish my coffee and set off for work. I usually take the bus and I've enabled an app for public transport routes on Net. It saves me time by identifying my location and automatically telling me the best transport options available at the moment. Right now, it's warning me that I should hurry up if I want to catch the next bus; otherwise I'll have to wait 20 minutes.

I don't want to be late for work so I run. My phone is in my hand, giving me updates on the bus location, and when I get to the stop it's just arriving. (My friends sometimes laugh at me because I'm still so attached to my phone. Of course, you could also receive the information through other means. But I'm still skeptical about wearable computers, and glasses just don't suit me.)

The biometric sensor instantly recognizes me so I jump right in and take a seat, and as we set off my mind starts to wander. I think about the time when we used to have paper tickets, before we had biometric face recognition. Thanks to the linkage of your biometric ID and Net account, it's a really handy way to authenticate yourself.

These thoughts, in turn, bring to mind the times before we had Net, when we didn't even have Internet. My grandfather sometimes tells me about how life was with no Internet. I don't remember. I don't think I was even born. But I still remember that when I was a kid there were plenty of social networks, search engines, online stores … you name it.

Then, suddenly, Net started to expand. In a few years it had conquered all the markets. Actually, originally, it had another name, and then it just changed to Net. It's an easy name to remember, though that's not really an issue. Since Net has no competitors, there's no confusion.

When I get to work the first thing I do is turn on the computer and connect to Net. Today, I have to send some messages to our providers about some purchase orders.

To check stock, I use an inventory management application developed by Net. We used to have some internal applications, but we switched to Net because it offers plenty of business applications, plus all the IT services we need (messaging, videoconferencing, storage, etc.). Our company is happy because we don't need to maintain them. Well, not exactly everyone in the company is happy. Our IT department is worried about all our data being stored in Net. But the Net system is just too cost effective to change it.

The downside is that since we migrated I need to maintain two different profiles in Net, one professional and one personal. At first this didn't bother me, but now I don't like to post too much information about my private life. Over time, I've become closer to some of my colleagues, and they've been added in my personal profile. It bothers me to think that the whole office can see pictures I put in my personal profile, for family and friends. I clean my profile from time to time to make sure everything is OK. But now is not the right time. I have to get back to work. I'll do it later.

It's almost time for lunch and I'm quite hungry. I need to order my food. I connect to the Net food delivery application. I can choose both the restaurant and the menu, or I can let them choose, based on my previous orders – in which case it will most likely be some dim sum or sushi. I usually take this option when I'm very busy, or just tired. It works well. In 15 minutes the food will be here.

While I'm having my lunch one of my teeth starts to ache. It seems I may have lost a filling in a back tooth. I need to make an appointment with the dentist, and quickly. I log into a Net app that shows me dentists in my area. Then I open the scheduling application. Great, there's one spot open for this evening, just after work. I haven't visited this dentist before, but nowadays it's really easy to change doctors or dentists because my entire health history is stored in a special medical record that I can send to the doctor or dentist I'm visiting.

I spend the afternoon working on the computer, writing messages to providers and clients, updating inventories … Like everyone else, I'm constantly connected to both profiles, so my friends' postings distract me. I get alerts every time someone writes me or updates their profile. I sometimes find it difficult to concentrate on my job, but if I don't stay connected I won't stay in the loop, because everybody is posting and answering in almost real time.

I'm done with my tasks for today, so I leave a little earlier and set off to the dentist. Again, the public transport route app comes in handy. When I arrive at the dentist everything is set. She checks me and reads my history, then decides to change my filling.

She also sees in my history that I get quite nervous about this kind of procedure. (Some previous dentist must have written that in my history, though I didn't know …) But she explains that it's a very easy intervention. And done in five minutes! Just ten minutes later, I receive a notification from Net saying that the cost of the appointment and the inlay has been deducted from my bank account. Good, something less to worry about.

When I get home I feel I need to rest a bit; actually I feel like reading. I usually rely on Net suggestions. This time Net's recommendation includes a book about safaris in Africa, which is strange because I never planned to go there or searched anything about it. Oh, now I remember. My friend Pablo used my computer for a couple of hours last weekend, when he came to visit. He said he wanted to go on holiday. He must have been doing searches on safaris. Didn't he use his own profile for the searches? Maybe mine was open? I can't remember. I buy a book about

dog breeds and training that Net has also recommended. Net systematically tracks my behavior so they know how busy my business schedule is. I had to cancel several dates with friends as well as my aerobic classes recently, for example. That's why Net has suggested that a dog would be great for a better work/life balance. They've been pointing out studies, making training recommendations, and suggesting nice dog walks. And I think Net is right. After getting the puppy, I'll ask Pablo, who also has a dog, what equipment and food he prefers, though I have to keep in mind that his advice may not be objective. After all, some vendors offer big discounts or even "freebies" if you recommend their products to other people.

Anyway, I'll read the books before I get the dog, so I'll be prepared. Sometimes I think I might be buying more than I need, but with all the suggestions and the instant recharging it's just so easy to buy things ...

The book is really absorbing and after a couple of hours I feel much better. I turn my laptop back on because I want to talk to my family. I also need to reply to a couple of friends' messages. I do everything through Net. Sometimes I wonder if all my correspondence and conversations are really private, but what can I do. This is what everyone uses nowadays, so there's no point thinking about it.

I can see that more and more people are becoming concerned, though. The government says they are ensuring that Net respects our data protection regulations, but I have my doubts about their ability to control how all the information Net collects passes between their apps, to their partners, advertisers, suppliers ...

Nobody really knows how they work internally, and they're not even located in the EU so I'm not sure how easy it is for our authorities to make them apply our laws. Besides, what could governments do: shut Net down? There are no alternatives. People would go crazy if they couldn't access the app for their favorite restaurants or to instant message their friends. Either you trust them — or you don't.

Actually, now that I think about it, some people don't use Net. There aren't very many of them yet, although they are becoming quite a crowd. Take my friend Marisa. She uses the Internet, but only to look for information; she has no profile in Net any longer. And she told me she didn't move out because she was worried about her privacy, but because maintaining her profile in Net — the constant updates, all the applications, the unwanted suggestions, etc. — was stressing her too much, and keeping her in front of the computer for too long. So she decided to cut it off. But I wonder how she does it. Nowadays, people even use Net to pay the electricity bill.

Another friend of Anna's, Simon, did not have a break from the Net voluntarily but thanks to a mismatch of data was forced to live without it for four months. Simon, a journalist focusing on foreign affairs, had been traveling a lot to crisis regions. He was also linked to a former

fellow student, now accused of being a member of a terrorist group. Net closed his profile until his background could be investigated in more detail. And despite recent European legislation that guarantees help for users in such circumstances within two weeks, Simon had to be much more patient. Without Net he couldn't even ride the bus. Anna couldn't pay for him because the facial recognition system automatically identified him and wouldn't let Anna buy a second ticket for a person without a Net account. Simon was more than relieved when finally his Net account was reopened.

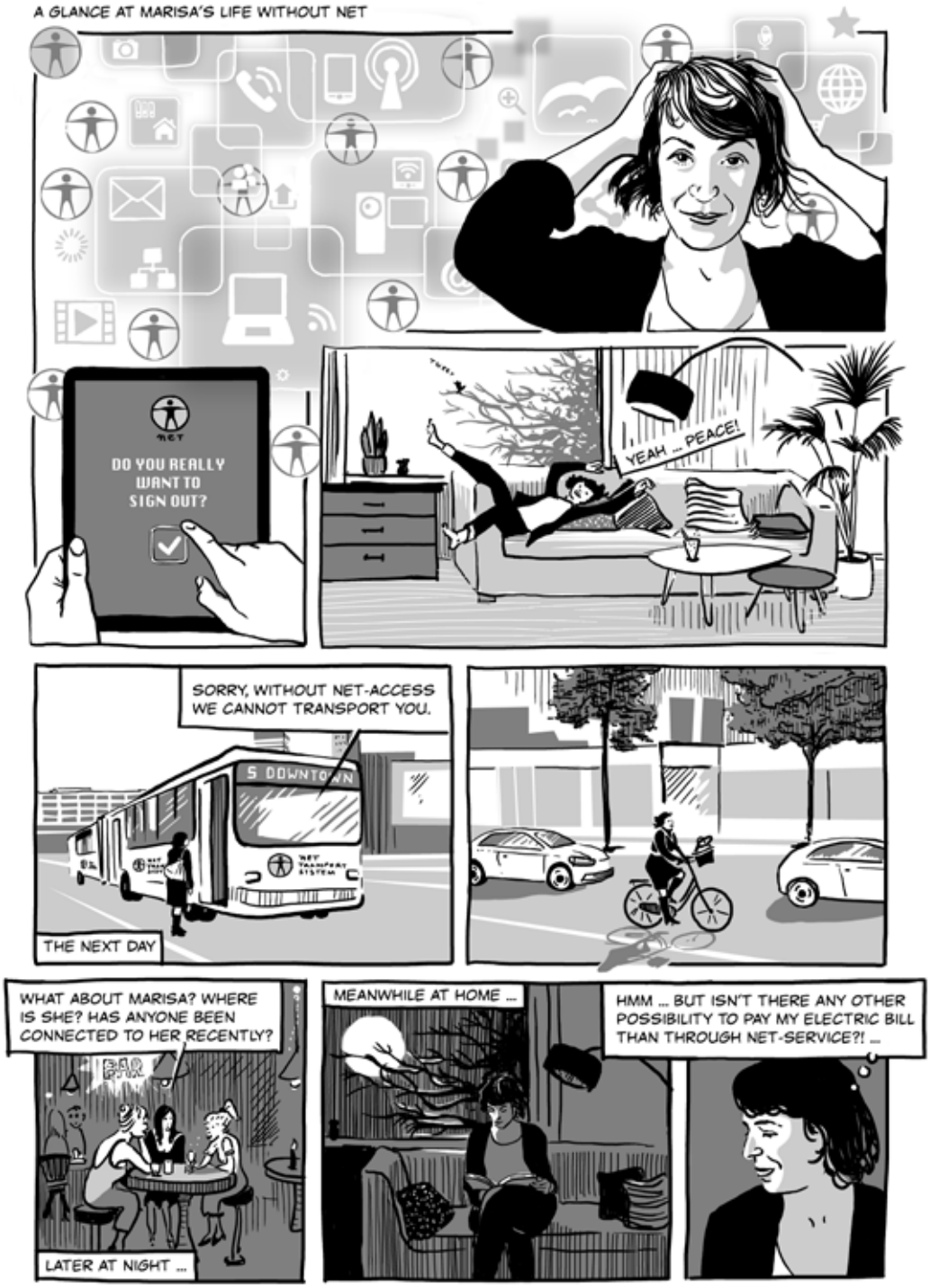
It's already 9 p.m. and I just remembered that I needed to complete an application to take French classes in the municipal language school. Again, I don't even need to enter the municipality website, because they've created an app for Net. It's convenient because they already have all my data (address, email, ID number, etc.), so I don't need to give that information again. They will reply to my account in two weeks to inform me if I have a spot for next semester. I've set an alarm in Net for all messages containing the word "Lessons," just in case I miss the reply.

It's been a long day. I'm quite tired and ready for bed. But first, I remember, I have to send a birthday message to my cousin Mercedes. So I go to her profile on Net and see to my surprise that in her public message board she has received a notification from her doctor. The clinic accidentally sent the notification, reminding her that her next appointment for dialysis is next Tuesday, to her public message wall!

I had no idea she was sick and she certainly didn't want anybody to know or my family would have told me. She must be really angry that this information was made public. I'm sure she'll contact the clinic and they will erase it immediately. But by now several people must have seen it, just like me. Should I ask her what's going on or just skip the topic? I don't know. I shouldn't have seen that message …

I realize this might happen to me, too; all my medical data are available online – though only for authorized medical staff, of course. Maybe I should check with my clinic to see if there's any way to communicate offline with them. But I'm not sure there will be. Most clinics have moved their appointment systems online, using the schedule management applications of Net.

Finally, I can go to bed. I feel like watching a movie. I enter Net movie store in my TV and I go to suggestions mode. Net picks a new popular comedy, because it thinks after a long day at work it will help me to relax and fall sleep. They're probably right, after all that's happened today!


A GLANCE AT MARISA'S LIFE WITHOUT NET
DO YOU REALLY WANT TO SIGN OUT?
YEAH ... PEACE!
SORRY, WITHOUT NET-ACCESS WE CANNOT TRANSPORT YOU.
5 DOWNTOWN
THE NEXT DAY
WHAT ABOUT MARISA? WHERE IS SHE? HAS ANYONE BEEN CONNECTED TO HER RECENTLY?
LATER AT NIGHT ...
MEANWHILE AT HOME ...
HMM ... BUT ISN'T THERE ANY OTHER POSSIBILITY TO PAY MY ELECTRIC BILL THAN THROUGH NET-SERVICE?! ...

EXPERTS' VIEWS ON SCENARIOS

DEMOSTHENES IKONOMOU is Head of the Information Security & Data Protection Unit at the European Union Agency for Network and Information Security (ENISA). From 1996 to 2008 he worked for DG Information Society & Media (INFSO) of the European Commission, principally in the management of R&D projects in the fields of wireless and personal communications, as well as networked media. In 2008 he joined the Technical Department of ENISA as a Senior Expert in the Security Tools and Architecture section.

His statement on identity:
Until recently behaviors in the online world were based on direct analogies to behaviors/situations experienced in the physical world. It is now apparent that the online world offers infinite new possibilities that are not based on our previous experiences in the physical world and where the role of identity is important.

"David's scenario (scenario 1) is more privacy-friendly while Anna's scenario (scenario 2) is an evolution of today's situation (with some consolidations taking place at industry level, and no intervention at member-state and/or EU level). I would like to believe that scenario 1 is most likely to happen since it is supposed to be less privacy-invasive, carrying embedded privacy features. Decentralization of resources and information also contributes to this direction, although I believe that this would not be enough to ensure privacy. In my view, privacy will be safeguarded by a combination of actions; for example, reducing the amount of personal data being communicated over networks to the absolute minimum required (scenario 1 also contains hints in this direction). In order for scenario 1 to become a reality, policy intervention at both member-state and (more importantly) at EU level would be required.

A characteristic of scenario 1 that I find particularly confusing, however, is that, at least in my understanding, the mobile device (smartphone) plays a very prominent role as an identity device, which in some respects goes against the idea of decentralization that is characteristic of scenario 1. Mobile device manufacturers have been working towards transforming the mobile device for personal identification (a smartphone is, by nature, a personal device). In my opinion a privacy-friendly set-up should favor the use of multiple IDs catering for different contexts, rather than a single ID linked to one device."

JULIET LODGE is Professor at the University of Leeds and a member of the Privacy Expert Group, Biometrics Institute. Her research focuses on biometrics, ICTs and human security, ethics and society, interoperability for EU internal and external security, PETs, privacy, border management and cross-border information exchange, communications, and eGovernance.

Her statement on identity:
Reliance on machine-readable identity tokens to relay personal data to allow or deny some of us access to services affects our understanding of identity, power, and accountability. What are the socio-legal and ethical implications for society of humans being hyper-connected, identifiable, and linkable by invisible robots making decisions for them?

"Scenarios 1 and 2 both imply a de-personalization of the individual where 'identity' as we know it seems to be replaced by the concept of a machine-recognizable code which, if it matches one known to the machine, allows something else to happen. In the scenarios, the something else is a human accessing a machine-mediated service. 'Identity' has become a snippet of an algorithm that can be associated with another code; in the scenarios, one attributed to a person. The scenarios are not about identity but identity management practices that allow 'services' to be sold to those who can use those systems and pay for their 'services.' Aspects of both scenarios

are likely to co-exist. Both raise critical ethical questions about the society created or that available to certain kinds of people. For example, consider the first scenario: this scenario raises profound ethical questions about the kind of society we are creating, and assumes that 'society' comprises individuals who are as educated, mobile, and affluent as he is. It follows from such an assumption that all individuals have the financial capacity to buy the technology and the associated services.

Does this imply full employment? Or is the implicit assumption that access to the 'convenience' posited in this scenario is to be available only to an elite? If, for example, the automated cars were available, would they only run on pre-selected routes where service providers could levy charges irrespective of their technical ability to run door-to-door? Would this discourage healthy lifestyles? Would children gain independence or would they become increasingly separated, by technological applications, from their parents? Where is the balance of 'goods'?

The scenario envisages many services that would be highly beneficial for disabled and socially isolated, infirm, or otherwise less privileged people. For example, the individualized transport system would improve the quality of life of the infirm and disabled by allowing them to access services independently instead of having to rely on costly 'social services,' in theory at least. However, would this simply mean displacing current costs and replacing, for example, human care assistants with equally costly e-services or robots, or e-health monitoring on mobiles?

The scenario foresees a paperless charging system: again convenient to the individual. It assumes personal control over sensitive data. However, has this society abandoned taxation? Are individuals and companies no longer required to retain records (paper based or e-records) for many years and to share them with government? What is foreseen in the event of technological failure, data degradation, loss, theft, etc. and full or partial outsourcing? The scenario also envisages a publicly owned automated car transport system. Is this realistic given the private-public sector partnerships that are so common?

Overall, this scenario offers a tantalizing vision of society and gives the impression that the individual is in 'control' of all aspects of his life, and has infinite and immediate choice, whether in terms of entertainment, leisure, travel, service access, and becoming aware of and buying goods. Yet all information is based on some pre-existing bias in its selection (by the provider) so how does the individual understand 'choice'? How does he make an informed 'choice,' and can he trust the provider to be honest, open, and transparent? Does fairness and dignity matter? It would be equally tantalizing to probe how critical infrastructure failures and other kinds of technical failures could upset the smooth life depicted, and contemplate what the implications would be for individuals and society of such 'failures,' determine who or what would be responsible for remedying failure, and who or what would deal with crises occasioned by such 'failures.'

Scenario 2: This scenario also raises profound questions about the kind of society envisaged and the nature of the autonomy of the individual. While Anna is more self-critical and reflective than David, she is still complacent and seems relatively unconcerned about the impact of Net on anything other than 'convenience.' Net directs her to convenient dentists and automatically

deducts costs: that assumes she has the capacity to pay. Does Net deny health care to those in need until they can pay? Does this allow Net to ration access to specific types of health care for specific groups of people, possibly depending on capacity to pay, age, skin or eye color, marital status, relatives, family, or government or business official ties? How could the overall system be misused and abused by malevolent or rogue insiders, governments, commerce, and anyone in a position to access and manipulate information or to use it to categorize and sort people into groups to be treated differently according to quixotic or capricious whims or the tyrannical predispositions of those in power?

Could such a system based on Net delivering 'convenience' be abused for commercial gain and exploited by monopolies inside the state/EU or by those who ultimately own them, probably outside the EU? What happens if errors occur in records, if they are mishandled, or corrupted through poor administrative procedures or poor storage? How are legacy records managed and rendered compatible? Does everyone have access to the same technologies and enjoy the same 'convenience' as Anna does? Or is she a member of an educated, able-bodied elite? Does she still enjoy human contact or is her life all online? Anna mentions the convenience of paying electricity bills automatically. This is a relic of what has been possible since the early 2000s. She does not mention smart meters and the control opportunities that these give to Net, although Anna assumes that she lives in a 'smart' environment where people take convenience for granted.

Anna asks the important question about life where individuals opt out of Net. But can they really do so and still engage in society? Can they still buy and access the goods and services on which their wellbeing depend? Or what are the conditions under which Net can deny them such access? Are such conditions known or arbitrary? How, in Anna's world, are the concepts of responsibility, responsiveness, accountability, and openness understood? Have they become irrelevant? Has democracy mediated by visible, electable human politicians become irrelevant?"

MICHAL KOSINSKI is Director of Operations for The Psychometrics Centre and Leader of the e-Psychometrics Unit. He is also a research advisor to the Online Services and Advertising group at Microsoft Research Cambridge, and a visiting lecturer at the Department of Mathematics of the University of Namur, Belgium. His current research is sponsored by Boeing.

His statement on identity: *My research shows that pervasive traces of digital behavior, such as Facebook® likes or browsing logs, allow the exposure of individuals' intimate traits. This raises important questions in regard to current technological and legal standards related to recording, storing, and processing user-related information.*

"In my opinion David's story (scenario 1) sounds more appealing and, luckily, seems to be more likely. There are a few mechanisms that I believe can protect us from the Orwellian and stifling reality of Net (scenario 2). First, I believe that national governments will strive to stay in relative control of information flows, financial systems, digital industries, and their citizens.

Hence, it seems that governments will have a low tolerance of various Nets, especially those completely out of their influence and control. There are numerous signs of this happening already, with China, Iran, and … the European Union actively fighting the US monopoly in search

and social networking. Second, while digital monopolies are arising much faster and are getting bigger, technological paradigms shift with increasing frequency, too, and digital monopolists fall even faster. Finally, I believe that just as many societies of today invest heavily in protecting human rights and democracy, societies of the digital age are going to treat privacy as one of the basic human rights. Consumer and political pressure in such societies has a potential to promote and foster privacy-preserving technologies and solutions.

A few things, in my opinion, will turn out differently from what is described in scenario 1. For instance, I think that there is going to be virtually no advertising in 2023. Advertising relies on broadcasting information about products and services in the hope of finding a receptive consumer. However, in my opinion the rise of personalized recommendation systems (which could be described as very highly targeted ads) and technological solutions allowing people to choose not to watch unwanted ads, are going to eradicate the pool of consumers receptive to such broadcasted messages and traditional marketing channels.

People will actively seek advice and recommendations, perhaps even paying for it, and are likely to ignore the broadcasted, crudely targeted marketing noise of today, which will soon disappear.

Also, I hope that in 2023 data will be stored in the cloud, perhaps in the encrypted form readable only with users' permission, rather than on local or mobile devices. I believe that local devices increase, rather than decrease, the risk of data losses, and expose their owners to data theft and scams. It might be much easier to attack large numbers of individual and relatively exposed devices than to attack heavily protected but still distributed online platforms with abundant internal and external firewalls.

Finally, I think that companies, e.g. railways or online stores, should and will be able to hold stores of transaction and user behavior data. However, those institutions may not be able to see who we are, as we will be hidden behind anonymous user IDs or avatars.

Online stores or social networks can be perfectly operational without the ability to identify their customers – user interactions, payments, deliveries, and warranty services can all be run in an anonymous mode. For example, any given institution (e.g. store) knowing only what is absolutely necessary to process the transaction (e.g. that anonymous user X paid for one of their products, which is to be delivered using a shipping company, which will obtain the delivery address directly from the user's X account, with his permission).

Privacy in the digital age is certainly an issue of utmost importance – perhaps as or even more important than energy sources. Freedom, democracy, social trust, personal and national security, and technological progress all depend on how we are going to shape our privacy-related policies and technologies."

Pablo García Mexía is Visiting Professor of Internet Law, The College of William & Mary, Lecturer at Masters Programs, Universidad Carlos III de Madrid and Professor of Internet Law, Universidad Internacional de La Rioja. He also acts as a Legal Advisor to the Senate of Spain.

His statement on identity: Big Data is causing a dramatic change in the way personal identities are handled, especially in the online world. As the Internet grows more central in human lives, rights as data protection are becoming increasingly important for industries, regulators, and citizens. New, more profound insights will be required to keep such rights effective.

"No doubt the first scenario would be the best option, since it is more respectful of identity and privacy. However I believe the more likely event will be a sort of mixture between the two, for some of the features of the first will be more probable to take place than the others and vice-versa, whereas some of the features on either side will likely happen not in full but only on a piecemeal basis. Thus:

1. **Regulation is likely to be strong**, even stronger than it is today, although the growing degree of data dissemination will make it increasingly difficult to implement. The French Data Protection Agency have rightly referred in this regard to a 'Big Other' scenario where not only big agents like governments or big businesses will be in possession of relevant personal information but simply anyone. Privacy may and should hence become the most fundamental and practical dimension of human dignity.

2. **Use of the Internet will already be widespread** by 2023 and not just limited to a couple of industry segments: I have been referring to this idea as 'the total Internet.' Borders between the digital and the analog environment, which are blurring today, might become almost imperceptible by then: 3-D printing is one of the most evident examples. The threat to identity will only grow, which should warn all of us as to the need to be much more cautious as we 'circulate' in the digital environment.

3. **Behaviorization** is actually personalizing all of us while consumerization is also empowering us in a whole variety of ways. This means our profiles will definitely be extremely accurate by then [2023], but our capacity to act autonomously as 'Internet citizens' and particularly as consumers will also be very notable. As a result we will have to stay alert in order to preserve the highest possible degree of control over our personal decisions.

4. Respect for **privacy and identity is a sound but also a smart business practice**. Recent events revealing opposite practices on the part of very notorious governments (some from outside of the EU) have proved that privacy-respecting European companies may end up being more competitive and more successful than their counterparts from across the world.

5. In a context as extremely volatile as the Internet it is **hard to imagine a world where only one social media provider might exist**. Rather, competition in that already crucial subsector of the digital environment has proved consistent enough until now, the existence of a few worldwide dominant providers notwithstanding (Facebook®, Google®, YouTube®, Twitter®...). The need to strengthen interoperability is nevertheless crucial, for in the end those providers still operate as separate 'silos' (Berners-Lee), while the risk of abuse from those dominant providers is gaining visibility. The right to data portability envisaged in the prospective EU-wide data protection regulation is a must in this respect.

6. **Open data (and open government) is the next big thing in eGovernment**, as is business intelligence (BI) in the commercial sphere. Yet as the British government has put it, it is government not citizens that ought to be transparent, while concerns among the public as to the growing threats to their privacy implied by BI are widespread even today. Privacy by design and privacy enhancement technologies (PETs) will turn out to be decisive in order to strike the right balance between the two extremes."

CONCLUSION

Foreseeing the Future — the Limitations

Our scenarios reflect the thoughts of two fictional individuals — David and Anna — on a single day in 2023. They have focused on aspects that seemed vital to us. We chose to omit many other aspects — notably, direct interaction with other people — not because we believe that technological developments will obviate the need for such interactions, but because we deliberately chose to restrict the scenarios' scope.

To what extent, however, can we foresee the future without simply extrapolating from the present? Who could have known ten years ago, for example, that people would become so inseparable from their smartphones? Or that seamless communications and travel would become so central to everyday life?

In our scenarios, phones or handsets are not simply communication devices but also a means to access different services and to identify the user. Yet by 2023 such devices may have been replaced by entirely new phenomena — wearable computers in clothing made from nanotech materials, for instance. We simply don't know. We can, however, indicate a range of thought-provoking possibilities. Consider, for example, what might replace advertising, which still plays a key role as a basic source of investment income in scenario 1.

First, though, let's take a look at some pros and cons of the world the scenarios describe from the end user's perspective. Our four selected experts have already mentioned others in their comments.

Scenario 1: Distributed Trust – But People Still Have to Use Their Power to Negotiate

In general, David's scenario sounds like a world where individual rights are respected, and where people profit from the services delivered by machines without losing control over their personal information space. David, after all, does not just seem to have few concerns about his privacy. He also has confidence in the technologies at issue. He trusts the automatic cars to bring him to where he wants to go, and he likes the fact that he can recharge them just about any-

where – and that the revolution in mobility is opening up new, tailor-made billing options. Indeed, by making people less dependent on one service provider, interoperability is forcing services and platforms to compete in offering the best user experience. However, interoperability remains a challenge and it is likely that in an interoperability-friendly environment, problems between certain providers and/or services remain and an exchange of all relevant information will not always work. Consequently, our personal information space will probably include more parts than we are aware of.

In a scenario where the integration of service largely uses a peer-to-peer decentralized approach, it is in general possible to have isolated service providers, isolated peers. Their business is to be disconnected from others for several reasons (privacy, independency, or hiding themselves from the others). As Stefano Rodotà, former president of the Italian Data Protection Commission and of the European Group on Data Protection, has observed, we are already experiencing the consequences of "dispersed" identity: "Information is entered in different data banks, each one of which returns a part or a fragment of the overall identity. We risk entering a time of identity "unknown" to the person concerned … in the sense that it [the identity] is found in different places, which may be difficult or impossible to know of, or to have access to."[2]

This also begs the question of what users should do who wish to remove their online identity. How can they remove "online skeletons" easily and be sure that no isolated, unintegrated "black holes" of personal data, unknown to them, remain?

Last but not least, even if the user had the option of switching networks, would they really be likely to do so? Is it not more probable that a combination of peer pressure and habit would induce them to remain with one provider?

Scenario 2: Centralized Control – a Trade-Off between Benefits and Surveillance

The key difference in this scenario is that a monopolist can do whatever it wants with my data and on my terminals. This has positive aspects, to be sure. In such a closed system, Anna knows who knows her and what is being shared about her. She also gets a great service. Since Net has a total picture of her, it can make relevant recommendations. What's more, since Net owns her terminal and can access her data it can install apps as a service that it thinks might be of interest to her.

However, the system also induces social conformity. People read the same books and watch the same movies. The end user is essentially passive. And if Anna opts out of Net, she opts out of social life.

In our scenario, Anna could have two profiles; but in such a centralized system this is unlikely to happen. Anna cannot live two different lives, because there is only one of her. Yet because her online behavior could give a false impression of who she is, Net could also have the "wrong" Anna.

---

[2] *see Stefano Rodotà's blog entries at www.identity-tower.com*

Indeed, dependence on such a monopolistic system could be very risky – especially if Net goes out of business. The financial crisis of 2008 has already shown us the pitfalls of assuming that some institutions are just "too big to fail."

The Likely Outcome

A mixture of both scenarios – combined with aspects we have not even considered yet – seems the most likely outcome. Or perhaps there will be a continual re-balancing or switching between the two situations – much as we have seen in regard to computer operating systems. So what effect will all this have on identity in the context of personal information space? Ultimately, it will be more difficult to "hide" aspects of one's personal information space, especially if we want the well-tailored and innovative products and services that rely on access to our personal information and behaviors. And as long as the trade-off between the irreversibility of the user's shared data and the services offered in return is transparent and proportional, this does not have to have negative consequences.

It is, of course, the role of business and government to ensure users' trust and confidence in service offerings. While working on the scenarios, the Task Force started to think about related (and much more complex) questions – to which they do not yet have answers. How, for example, is my online identity evolving when I am disconnected from it? As long as I am continually "feeding" my online life, both it and my "real" life will mirror each other. But what happens when the two identities – real and virtual – are disconnected for a long period of time? What happens when my online identity is restored? How can I monitor it when I am not connected and attending to it? Can I create a sort of watchdog? And what happens when I cannot monitor it anymore – when I die, for example? We hope this publication will stimulate further discussions about the impact of machines on our lives, and the implications for such concepts as privacy, control, choice, autonomy, and communication.

TASK FORCE PARTICIPANTS

Katja Crone

Her statement on identity

"Persons not only exist as objects across time, they also have an understanding of their existence across time. Clearly, the notion of identity is linked to our self-understanding as individuals in various important ways. I am particularly interested in clarifying different meanings and uses of 'identity' and their relations to each other."

Katja Crone (Dr. phil.), is assistant professor at the Institute of Philosophy, University of Mannheim. Previously, Katja Crone taught at Humboldt-University Berlin (2008–2012), at the Martin-Luther-University Halle (2006–2008), and at the University of Hamburg (2000–2002). She worked as a research officer at the German National Ethics Council from 2002 until 2006. In 1999, she was a research fellow at King's College, London. She studied philosophy and German Literature at the University of Hamburg and at Université Paul Valéry, Montpellier. Katja Crone has published numerous articles on topics in the philosophy of mind, especially on subjectivity, personhood, and consciousness.

Enrico Frumento

His statement on identity

"Two important topics are tied with the evolution of identity: wearable electronic systems and the flourishing of multiple online identities. Wearable electronics need new approaches to the design, because for the first time fashion, technology, physiology, and psychology are all involved in designing convincing products. Designing wearable systems needs a tight integration of competences among electronics, psychology, and design. At the same time, most people have multiple identities, one only of which is real and all the others digital, often not all coherent or representative of the 'real' person. The revolution of wearable electronics is to bridge the digital and physical worlds and connect different identities: what starts 'virtually' could become physical and vice versa. This collapsing of digital and real identities, of real bodies and virtual personalities, fosters big challenges."

Enrico Frumento is a Senior Specialist at CEFRIEL (ICT Centre of Excellence for Research, Innovation, Education & industrial Labs partnership). Enrico Frumento's research activity started at CEFRIEL in the field of e-health service and telemedicine systems. Over the past four years he has gradually moved his interests towards wearable electronic systems and security. Thanks to his participation in several European projects he gained experience in the design of wearable electronic systems and body sensors. He also recently co-authored the Italian book "IndossaME: il design e le tecnologie indossabili" (IndossaME: design and wearable electronics), with Canina M. et al. (Franco Angeli Editor, Jan 2010). In the field of security he currently contributes with his research on Secure Code Development Techniques and hacking/cracking techniques and

malware analysis (Reverse Code Engineering and Code Hardening). Thanks to his recent collaboration with the Milan Department of Cognitive Science his studies have been extended to include Social Engineering and the problems tied to the definition of identity in the Web era.

Clara Galan

Her statement on identity

"Our identity, or at least how we are perceived by the rest of the world, is being challenged by current technological developments. A parallel identity has emerged in the online world. It reduces distances and improves our ability to interact with others. However, to be able to set boundaries, to feel we have control over what is known about us and how it is used, is becoming a great concern for many."

Clara Galan is an information technology officer of the Spanish National Administration. Since 2008 she holds a position as Cell Head for systems security in the Information Technology Department of the Spanish Ministry of Defense, where she is responsible for elaborating security policies and defining security requirements of information systems. In the past, she has been a seconded national expert in the European Union Agency for Network and Information Security, where she worked in the area of privacy and trust. She graduated with a Telecommunications Engineering degree from the Polytechnic University of Madrid. Since then, she has concentrated on the field of information security, with a special interest in secure eGovernment services and data protection.

Gisela Meister

Her statement on identity

"State-of-the-art smart cards as electronic identity (eID) cards can already be used for a visual and electronic verification of the citizen's identity. Their electronic interface provides technical interoperability as well as privacy protection. The use of such eIDs as representatives of personal identity should be discussed from social and economic perspectives."

Dr. Gisela Meister is Giesecke & Devrient's Standardization Director, coordinating all standardization activities within G&D. She is also the Head of R&D's Technology Consulting Department, which includes responsibility for G&D's security evaluation projects. Gisela Meister has been employed with G&D since the end of 1989. She chairs the European standardization working group for digital signature applications on smart cards and actively contributed as Task Force Convenor to the development and harmonization of the European Citizen Card Technical Standard within CEN. Since 1994, Gisela Meister has been a member of the DIN national committee on Card Standardization and since 2006 she has been chairing the technical committee NIA 17.4 and acts as head of the German delegation of its international mirror technical committee within ISO/IEC.

Gisela Meister holds mathematics and economics from the University of Münster, received the SIT Fraunhofer Smart Card prize 2004, and is a member of several program committees regarding smart cards and security aspects, such as the BSI IT-Sicherheitskongress in Bonn, the Fraunhofer Smart Card Workshop in Darmstadt, the Chip to Cloud Conference in Nice, and the ID World symposia in Frankfurt.

Daniel Nagel

His statement on identity

"Who one is is always a matter of having adopted certain masks of identity reflected from the world as offers of who one could be in the world (M. Eldred). Grasping this multifaceted character of identity and the resulting interplay between free self-determined selves is intriguing both in a legal, philosophical, technical, and sociological sense."

Daniel Nagel is a member of the IT Law Department of BRP Renaud & Partner. He focuses his practice on online and offline privacy issues, data security, and international law. Daniel Nagel is a permanent contributor to the Austrian UN CISG database, a member of the Jean Monnet European Centre of Excellence, University of Leeds, and a fellow of the Tech and Law Center, Milan. Daniel Nagel studied law at the University of Heidelberg, the University of Innsbruck, and at the University of Leeds. He has published numerous papers in the field of privacy and co-authored the book "Digital Whoness: Identity, Privacy and Freedom in the Cyberworld" with M. Eldred and R. Capurro.

Anton Stölzle

His statement on identity

"Identity is the core. For people, identity outlines how we are viewed by others. For things it is key for communication and interaction in complex networks. Identity is developed through communication and interaction, but with the rise of the Internet this process is complicated to manage. There is a need to really understand what it is and how it is developed and applied."

Anton Stölzle is Group Vice President Research and Development in G&D's Banknote Processing department. Before he joined G&D in 2007, he was Head of Development Portable Monitoring at Tektronix in Berlin and, until 2005, Head of Wireless Development Nortel Networks Germany, where he was responsible for intelligent networks for mobile communication, feature development for mobile core networks, lawful interception, and the coordination of multinational software development projects. Anton Stölzle graduated as an Electrical Engineer from the Technische Universität München with special emphasis on communication technology and cybernetics. He subsequently went to U.C. Berkeley to complete a Master of Science in Electrical Engineering and Computer Science and obtained his PhD on the topic of "ASIC System for Real Time Speech Recognition."

Daniel Trottier

His statement on identity

"Digital and social media increasingly shape our identities. Our enthusiasm for these services is rivaled only by our unease and uncertainty about their impact. Not only do they increasingly monopolize our identities, but they render us visible and searchable in ways that warrant critical scrutiny."

Daniel Trottier is a postdoctoral fellow at the Communication and Media Research Institute (CAMRI), University of Westminster. He previously held postdoctoral fellowships in the Department of Sociology at the University of Alberta and the Department of Informatics and Media at Uppsala University. Daniel Trottier obtained his PhD in the Department of Sociology at Queen's University, Canada. His current research considers the use of social media by police and intelligence agencies, as well as other forms of policing that occur on these platforms. As part of this research, he is participating in EU-funded projects (http://respectproject.eu/ and http://www.projectpact.eu/). Daniel Trottier has authored several articles in peer-reviewed journals on this and other topics, and published "Social Media as Surveillance" with Ashgate in 2012. He has also published "Identity Problems in the Facebook Era" with Routledge in 2013, and is completing an edited collection with Christian Fuchs entitled "Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube," to be published by Routledge.

Rigo Wenning

His statement on identity

"There is too much confusion between identities and identifiers. The Internet and the Web would not work without unique identifiers. They identify resources, devices, things – not people. Many consider identity the instrument of power and control in the globalized and networked world. Many believe controlling identity will generate trust for e-commerce. I don't. Identities are a matter of convenience and imagination for social interaction. Build your identities, don't have them built. We have to provide the tools for the people, not the identity prison that puts every person into a machine-readable bucket."

Rigo Wenning is the legal counsel of the World Wide Web Consortium (W3C), chairing Patent Advisory Groups, representing W3C at the EC's Mulitstakeholder Platform, and overseeing all legal and contractual aspects of the work of the Consortium. After first steps on the Web as early as 1993 during his research at the Institut für Rechtsinformatik at Saarland University, Rigo joined W3C in 1999 to work on Privacy and P3P. Rigo Wenning participated in the FP7 projects PRIME and PrimeLife that did research on next-generation identities management. He has organized many workshops on privacy enhancing technologies and is deeply involved in W3C's Tracking Protection Working Group, which works on the "Do Not Track" technology.

PUBLISHING INFORMATION

Contact
Giesecke & Devrient GmbH

Fabian Bahr, Head of Berlin Office
Phone: +49 (0)30 2009 5480
fabian.bahr@gi-de.com

Mareike Ahrens, Project Manager
Phone: +49 (0)30 2009 54812
mareike.ahrens@gi-de.com

Design: Havas Worldwide Munich

Comic strips: Studio Nippoldt

ISBN: 978-3-00-044225-4

November 2013
Printed on FSC®-certified paper using a carbon-neutral process