
DMC

By David Wright,
Michael Friedewald,
Wim Schreurs,
Michiel Verlinden,
Serge Gutwirth,
Yves Punie,
Ioannis Maghiros,
Elena Vildjiounaite, *and*
Petteri Alahuhta

THE ILLUSION OF SECURITY

A fictional scenario of daily life in a world networked with ambient intelligence illustrates the dark side of the technology and the need for appropriate safeguards.

While most stakeholders paint the promise of ambient intelligence (AmI) in sunny colors, there is in fact a dark side to AmI. In a way, this dark side is inherent in the very nature of AmI. Intelligent networks embedded everywhere will enable data aggregators to acquire a lot more personal information, far more than in today's world, greatly magnifying the risk of abuse of that data.

Illustration *by* John H. Howard

Most AmI scenarios illustrate its benefits. The dark scenarios, developed by the SWAMI (Safeguards in a World of Ambient Intelligence)[1] project, are different as they point out the risks that must be mediated if AmI is to be a future success story.

The scenario we present here hinges on the theft of data from a multinational company. The company suffers from the illusion of security—that is, the belief it has implemented more than adequate security measures—only to discover it has not.

A Dark Scenario

The Data Mining Corporation (DMC) has an almost perfect business model. It collects data about individuals from hundreds of sources and then sells the aggregated data back to many of those sources. Its principal sources (and clients) include insurance companies, retail chains, media conglomerates, credit-reporting agencies, mobile phone companies, law enforcement agencies, customs and immigration authorities, and intelligence agencies.

Among the ways DMC has managed to sidestep legislative and regulatory constraints on transfers of personal data is through mergers with or acquisitions of companies with their own extensive databases. DMC is headquartered in Miami, but now has major subsidiaries in London and Tokyo. It is listed on the New York and London Stock Exchanges and is considering a listing on the Tokyo Stock Exchange.

Scene 1: Management board meeting. The company secretary stands close to the iris scanner. The door opens and he enters the boardroom. The president, already there, nods a slight greeting to the company secretary who can see his boss is preoccupied. She is watching the boardroom video display, which depicts her vice presidents coming down the corridor toward the boardroom. A few seconds later, the vice presidents enter one by one and take their seats.

"Okay, let's get on with it," says the president. "Show the agenda." The agenda appears on the large wafer-thin video screen on the wall opposite the president. Three items are listed:

- Data from developing countries. (Switzer)
- Theft of data. (Perrier)
- Considerations re: listing on the TSE. (Hausmann)

Kevin Switzer, vice president for operations, speaks. "We've had complaints from the Customs and Immigration folks about the shortage and reliability of our data on people coming into the States. It mainly concerns people from developing countries. With our profiling technologies, we are able to identify anyone who might be a security risk or disposed to anti-social behavior. Unfortunately, most developing countries have no AmI networks, which makes it impossible to build up the same kind of detailed profiles of individuals like we can here in the U.S., Europe, or Japan. So the immigration authorities have been making threatening noises about refusing entry to people from countries without AmI networks." Switzer seems concerned, but then smiles. "I think we have a golden opportunity here. We can set up AmI networks in those countries as long as we are the ones to collect and process the data. You'd think most countries would jump at the chance to have networks put in place at virtually no or little cost to them, but some of the countries are quibbling with us."

"Quibbling?" asks the president, "What do you mean?"

"Quibbling about control of the data. They say if we control the data, it's tantamount to signing their sovereignty over to us. But we've been working on a deal where we copy for them the data we collect... well, some of it, at least. Our intelligence agencies would not want us to hand over everything, nor do we have to. We can offer the raw data to the developing countries, but they won't know if or how we've processed the data, especially since we do the processing here in the U.S. or in the U.K., outside their jurisdiction. They'll have to settle for what we give them."

"Okay, that sounds good to me. Any objections?" she asks the others, who remain silent. "No? Okay, then, Jacques, it's your turn. What's the latest on the theft at our London office?"

Perrier, vice president for security, shifts uncomfortably in his chair. "Well, as everyone here knows, we have a regular monthly audit of DMC's data processing activity. From the last audit, we discovered that there had been a second back-up of data immediately after the first, but we can't identity exactly the device to which the data was backed up..."

"But you know *who* made the second back-up?" asks the president.

"Umm... uh... yes. It seems likely that three of my staff were responsible for doing the regular back-ups that night. We want to ask them about this second

[1] For a detailed version of this scenario and for three other dark scenarios, see D. Wright, S. Gutwirth, M. Friedewald et al., *Safeguards in a World of Ambient Intelligence*. Springer, Dordrecht, 2008. The project was funded under the European Commission's Sixth Framework Programme. It had five partner organizations, represented by the authors. The project aimed at identifying a range of safeguards to the threats and vulnerabilities facing privacy, identity, security, trust and inclusiveness from ambient intelligence. The views and opinions expressed in this article are those of the authors alone and in no way are intended to reflect those of the European Commission.

back-up, of course, but we haven't been able to contact them. It seems all three left on holidays a few hours after the second back-up was made. They were supposed to have returned three days ago, but they haven't reported for work and they haven't answered our calls."

The president is getting angry. "And why don't you know where they are? Surely you can track them via their location implants. Everybody has to have a location implant. It's a condition of employment in our company, just like any critical infrastructure like banks or nuclear power companies."

"Yes, but their implants are inoperable. They could have been surgically removed," says Perrier.

"And what about the sensor networks in their homes and cars?"

"Yes," says Perrier. "Like other employees, they've agreed that we can check their home systems and we've done that. There's obviously nobody in their apartments, and their cars have been stationary since they left on holidays..."

"Have you checked the surveillance systems?" asks the president. "You can't go anywhere in London without being caught by surveillance cameras hundreds of times a day."

"Yes, we've been reviewing the data from the surveillance systems, too," says Perrier. "But they haven't shown up on those either. We've also checked with the airlines and railways and car rental agencies to see where they might have gone. Now we know they left for Costa Rica, but then the trail goes cold. As Kevin has just pointed out, the developing countries don't have the kind of AmI infrastructure needed to track people, so they could really be anywhere. We've also been checking with the 4G companies, but so far, there's been no data recovered on use of their mobiles."

"I don't understand how they could have got past our own security systems," says the president. "We have access control to prevent unauthorized employees from copying or manipulation of data."

"That's true," says Perrier. "The snag is that *they* were authorized. Quite a few employees have partial access, so if three or four with access to different bits collaborate, as these three appear to have done, they are able to get virtually full access to the data."

"Even so," says the president, "how did they get the data outside our headquarters?"

"With today's technology, it's easy to copy vast amounts of data in seconds onto high-capacity optical storage devices no larger than a deck of playing cards, which makes them easy to conceal on the way out of the building. It's hard to break into DMC offices, but it's not hard to get out."

"If we were exposed, it would be a complete disaster," says MacDonald, the VP for public affairs. "Among other things, it would show our clients that the profiles of our own employees are not reliable because we weren't able to predict that these few bad apples were going to abscond with copies of our records."

Max Court, DMC's general counsel, speaks up. "If we were exposed? Are you suggesting we should withhold information about this theft from the police and those whose files have been copied?"

"Of course," says MacDonald. "It's obvious, isn't it? I'd hate to imagine what it would do to our share price and our plans for a listing on the Tokyo Stock Exchange."

Scene 2: The Old Bailey, two years later. BBC1 news anchor: "And now we go to our reporter, Miles Davenport, who's been at the Old Bailey today, attending the trial involving the Data Mining Corporation and its directors. What's the latest, Miles? Has the jury returned with a verdict?"

Miles Davenport: "Thanks, Serena. No, the jury hasn't returned yet, but an announcement is expected in the next few minutes."

BBC presenter: "Miles, can you just recap for our viewers what this trial's been all about? And why is it so important?"

Miles: "Sure, Serena. It all started two years ago when *The Financial Times* broke a story about the theft of personal information on about 16 million people in the U.S. and the U.K. All this data was held by DMC, the world's largest data miner. DMC discovered that someone had broken into its supercomputers but it didn't say anything to anybody.[2] Then there was a big spike in the number of identity theft cases. People were seeing all kinds of purchases on their monthly statements for things they hadn't bought. A lot more people and companies were reporting that they were being blackmailed with threats of releases of embarrassing information. The FT got wind of this, and was able to trace the source back to a theft of data from DMC.

"At first, DMC denied everything, and then said they wouldn't comment on it because the theft was under investigation. When its share price began skydiving on Wall Street and in London, DMC had to call off plans for a listing on the Tokyo Stock Exchange. For awhile, it looked like DMC was going bust, but the U.S. government stepped in and

[2]DMC is not alone. See J. Krim, "Consumers Not Told Of Security Breaches, Data Brokers Admit," *The Washington Post*, Apr.14, 2005. See also D. Stout and T. Zeller Jr., "Agency Delayed Reporting Theft of Veterans' Data," *The New York Times*, May 24, 2006.

propped up the company. They said that national security was involved, and they could not allow the company to go bust."

BBC presenter: "Personalized services are great, of course; they save us lots of time. And so are the improvements in our security, like knowing when we are near criminals or suicide bombers, but isn't there a dark side?"

Miles: "Well, yes, there is. We have to trust companies like DMC to keep our data safe, secure, and accurate. But now we know that our data is not secure. DMC not only failed to protect our data, they were actually selling it to governments who were hunting for people with behavioral dysfunctions in case they were likely to commit a serious crime or an act of terrorism. They've also been selling the data to other companies who were using the data to spam just about everybody in the U.S. and here in the U.K. DMC claimed they couldn't be held responsible for what their clients did with the data." [3]

BBC presenter: "Thanks for that recap, Miles, but weren't there some other issues that came out during the trial?"

Miles: "There certainly were, Serena. People are entitled to see their records, but most people didn't even know about DMC, let alone the fact that they had built up such extensive records on every one of us. So, some consumer activist groups banded together to sue DMC for negligence. People had no idea just how pervasive ambient intelligence had become. We heard that in many instances the data coming from so many different ambient technology networks was often in conflict or didn't make any sense. DMC countered that its proprietary software contains an algorithm for comparing data from different sources to maximize reliability and its predictive capability, but under intense questioning from the prosecution, they admitted they could never eliminate unreliability nor could their predictions of who might be a terrorist or criminal be 100% certain."

BBC presenter: "And the DMC directors, what's going to happen to them?"

Miles: "We'll find out after the jury comes back with the verdict. The DMC president, however, has already resigned, but she went out with a golden parachute—a severance package worth a cool $100 million—and now she's apparently living in Costa Rica."

[3]cf. W. Safire, "Goodbye To Privacy," *The New York Times*, April 10, 2005: "Of all the companies in the security-industrial complex, none is more dominant or acquisitive than ChoicePoint of Alpharetta, Ga. This data giant collects, stores, analyzes and sells literally billions of demographic, marketing and criminal records to police departments and government agencies that might otherwise be criticized (or defunded) for building a national identity base to make American citizens prove they are who they say they are."

Analysis

Here, we present a methodological structure for analyzing this scenario, which could also be applied to the construction and analysis of many technology-oriented scenarios.

Situation. The objective of this scenario is to depict what is called the "illusion of security" in an AmI world a decade from now, when ambient intelligence has become pervasive in developed countries (but not developing countries), when most people embrace the personalization of services and the supposedly enhanced security resulting from the application of AmI. Although AmI offers powerful new technologies for security applications, such technologies can be undermined by determined people.

This dark scenario is a trend or *reference scenario* because it starts from the present and projects forward on the basis of to-be-expected trends and events. It is intended to be realistic or descriptive rather than, for instance, normative or extreme.

The scenario concerns the theft of personal information held by a data aggregator (DMC) by three rogue employees. Theft of identity occurs now, but the difference between such crimes today and in the future is the scale of the data involved. AmI will make it possible to gather orders of magnitude more information about virtually every person in America, Europe, and Japan. The future is also marked by an increasing concentration in the control of personal data. Thus, the risks to individuals are much greater when something goes wrong.

AmI technologies used in the scenario. The scenario makes reference to several AmI or AmI-related technologies, including:

- Biometrics, such as the iris scanners that grant admission to the boardroom;
- Networked sensors/actuators, such as those that detect human presence in cars or homes;
- Speech recognition and voice activation, such as the system in the boardroom that recognizes a command from the president of operations to show the agenda;
- Surveillance technologies including video cameras, keylogging software, location implants, biometrics, and networked sensors, that are used to monitor where employees are and what they are doing;
- Intelligent software that can analyze past behavior and preferences in order to predict needs and personalize services (which TV program to watch, which products to buy), something Serena, the TV presenter in Scene 2, views as welcome by the market;

- Networked RFIDs, sensors, and actuators for gathering data about people and the products they have or services they use. These and other AmI technologies greatly facilitate profiling of virtually everyone; and
- Fourth-generation mobile phones, which combine today's PDA capabilities with third-generation mobile technology (and much else). Such multimedia personal devices provide a wide range of services (and collect vast data), but 4G networks are not available everywhere, especially not in developing countries, like Costa Rica, to which the data thieves and, later, the DMC president decide to decamp.

Applications. The AmI technologies referenced in the scenario are used in various applications, including:

- *Security:* DMC has instituted various security measures, such as access control (to offices and software systems), key logging, proprietary software, employee monitoring and so on, to ensure the security of the personal data it collects and processes.
- *Surveillance:* Video cameras and other surveillance technologies keep watch on virtually everyone, especially in the streets and shops of London (and other cities), but increasingly in their homes too. Such technologies can be used to detect whether someone exceeds the speed limits or pilfers items from the shops, but also whether they engage in terrorism on the Underground.
- *Immigration control, counterterrorism and policing:* AmI networks are used to compile personal data and profile would-be visitors and immigrants to help officials assess whether they present a security risk or might behave in a socially dysfunctional way.
- *Personalization of services and targeted marketing:* With the prevalence of AmI networks, and the vast amount of personal data they generate, service providers can individuate their services to new levels of specificity.
- *Critical infrastructure protection:* It's hard to get into the DMC offices (but not so hard to get out). AmI sensors and actuators, biometrics, and other access control measures are used to protect critical infrastructure, such as DMC, banks, public utility networks, government offices.

Drivers. The drivers at work here can largely be derived from the motives and needs of the principal characters in the scenario and/or economic, political or social forces. DMC's management are primarily driven by the profit motive, a desire for scale (such as to be the market leader, to swallow or overwhelm competitors) and to create a situation where their clients are dependent on DMC services and products.

A second driver must be market demand, that is, there are many companies and governmental agencies that want the processed data that DMC has been supplying.

A third driver, not so dissimilar from the first, is that the data thieves are also impelled by the profit motive.

A fourth driver is respect for the law. This is (partly) indicated when DMC's general counsel expresses some disbelief at the suggestion that DMC should cover up the data theft from both the police and those whose files have been copied. In Scene 2, respect for and redress through the law is the key driver.

Yet another driver can be identified, such as the media's desire for a good story, which has the benefit of raising public awareness about the pervasiveness of AmI.

The scenario raises several issues:

Digital divide. The developed countries have AmI networks and the developing countries don't. There is a risk that this will lead to discrimination against developing countries. Intelligence agencies and immigration authorities may not admit visitors and emigrants from countries without the AmI networks needed to generate detailed profiles and a determination as to whether a person could be a security risk. The digital divide issue radiates in many directions and prompts many questions. Will the quest for perfect security really protect our societies? Recent developments suggest we are as much at risk from homegrown terrorists as from those in developing countries. Also, if immigration is restricted from developing countries without AmI networks, won't our "developed" societies somehow be impoverished because we will lack the views and experiences of those who know what it's like to live on both sides of the digital divide? If immigration is restricted, especially on the grounds of a lack of AmI-generated data, won't we inflame resentment in developing countries?

Concentration of power. DMC is the clear market leader in the aggregation and processing of AmI-generated data. It has a wide range of powerful clients. When there is a risk that DMC might collapse, the government steps in to prop up the company. When governments and client industries are so dependent on a single market player, they are at risk of being held hostage. Even if the company professes respect for the law, there is a distinct risk, whatever its declared inten-

tions, that it will act in a monopolistic way ("Power tends to corrupt."). High technology companies may fly under the radar screen of competition authorities for a long time before they are noticed, by which time they may have, like DMC, accumulated too much power.

The concentration of power manifests itself in other ways in the scenario. DMC says it is willing to establish AmI networks in some developing countries as long as DMC controls them. Developing countries, concerned about their sovereignty, will "have to settle for what we give them," says Switzer. Also, employees have "agreed" that DMC can check their home sensor networks, that is, if they want a job at DMC, they must agree. Similarly, employees must bear location implants.

Lack of public awareness. Despite the convenience of personalized services and enhancements in security made possible by AmI, most people have not comprehended just how pervasive AmI has become, nor of the scale and volume of data being generated about them by AmI networks. In the scenario, public awareness is increased as a result of the investigative reporting and media coverage of the theft of data from DMC, the resulting trial, and the high-level political intervention to stave off DMC collapse. Aroused public awareness may force changes in legislative or regulatory oversight. Hence, public awareness and the pressure of public opinion, stoked by the media, have utility as a safeguard against abuse. Unfortunately, such pressure is almost always reactive.

The illusion of security. Most people are willing to trade some of their privacy for better security. The scenario suggests that terrorism has become sufficiently serious that the intelligence agencies and immigration authorities are becoming unwilling to admit foreigners unless they have detailed information on each individual. Similarly, DMC employees seem willing to have location implants and surveillance equipment installed not only in their offices but in their homes and cars. They probably see this as beneficial in security terms.

It is ironic that DMC and its directors face a class action lawsuit on the grounds that they were negligent in securing personal data. Security would seem to be one of DMC's key strengths, one of its key selling points. DMC can hardly believe that its many security measures—video surveillance, biometrics, key-logging software, access control measures, regular audits, employee implants and so on—could fail. But the question is: have DMC executives done enough? Was their profiling of employees sufficiently rigorous so that they did not need to fear theft by insiders? We are told that it was difficult to get into DMC offices, but not difficult to get out. DMC's security defenses seemed primarily aimed at preventing breaches at its perimeter.

The company was rather less focused on the enemy within, hence the three employees (who had authorized access to the data) were able to collaborate, to copy the files and exit the premises without being challenged. Further, it seems to have been relatively easy for them to remove their location implants and to disappear without a trace. But the three employee data thieves are not the only miscreants at DMC. The senior executives also behaved unethically and illegally by not informing the police and their customers about the data theft.

Hence, we can conclude that an illusion of security prevailed at DMC and, perhaps, more widely within society as a whole. The illusion is fed by the implicit assumption that various AmI technologies and procedures will form an adequate defense against miscreants. Unfortunately, no matter how strong these technologies and procedures may be, they may still fail, especially against insiders acting in concert (both the employees and the executives).

At the societal level, we may assume that laws and regulations will protect us, but this scenario suggests that even there we suffer from the illusion of security—it takes a class action suit to bring DMC to justice. Market forces that might otherwise punish DMC are undermined because government decides that DMC cannot go to the wall. DMC has managed to acquire so much power—partly through its proprietary technology and partly through its market dominance—and has come to play so big a role in (ironically) national security that government cannot allow it to go under. But if DMC was unable to detect the security risk posed by three of its own employees, isn't the government's confidence in DMC technology misplaced?

The illusion of security is also fed by unwarranted trust. The issue of trust is not directly raised in this scenario, but it is not far away. One would think that a data aggregator, processor, and reseller like DMC would have some obligation to inform people whenever it sells data to others or takes over another company with personal data records. But this has not occurred. It seems that DMC clients, the intelligence agencies and immigration authorities, are content that individuals are not informed about what information DMC has on them, even if the law dictates otherwise.

California and a number of other states have strict laws requiring that companies do inform individuals

when their data has been compromised—but that does not mean that they *will*. Compliance will depend as much on corporate culture and, especially, ethics as on legal deterrents. Thus, to some extent, even laws and regulations can instill an illusion of security.

Conclusion

The principal conclusion we draw from this article—from the dark scenario and the analysis—is that, although we can expect amazing advances in the development and deployment of ambient technologies, there is a risk that corporate ethics in the year 2018 will not be so different from those prevalent in the year 2008, which is to say that some companies will be good corporate citizens and some won't. Similarly, some companies will have rogue employees just as they do today who are capable of undermining what might be perceived as strong security (technologically, procedurally, legally). A principal difference between today's world and that depicted for the year 2018 could be that security concerns about terrorism and antisocial behavior will be such that unless individuals have really detailed profiles compiled from data from AmI networks, they may be barred from entering a developed country. Also, while people may welcome the convenience from personalization of services and the ubiquity of surveillance technologies, they may be lulled into a false sense of security.

As mentioned in the introduction to this article, there have been few "dark" scenarios put forward by AmI experts and aficionados. The SWAMI project has taken a deliberately contrarian position with regard to scenarios that show the "sunny" side of AmI. While the authors are as enthusiastic as anyone about the potential of AmI, advances in surveillance technologies, biometrics, and fourth-generation mobile systems, they believe the AmI community, policymakers, and society must be alert to possible abuses of the technology. Constructing scenarios and using an analytical structure along the lines as noted in this article offer a useful way of stimulating dialogue about such possible abuses as well as other technology issues.

Identifying possible abuses is the first step in devising safeguards. Almost certainly, a mix of safeguards will be needed—technological, socioeconomic, legal, and regulatory and even cultural safeguards can be envisaged.[4] As a minimum, the SWAMI consortium advocates a privacy impact assessment for any projects supported by public funding. Designers of new technology should be required to factor in data protection in any new AmI architectures and networks. Legislation and regulation will probably be necessary, and one can predict that will elicit protests from those in favor of deregulation and getting the government off their backs. So be it.

If civil liberty advocates have had concerns about encroachments upon our privacy in the emerging surveillance society, they will be positively apoplectic if AmI, already being implemented in a somewhat piecemeal fashion, becomes as pervasive as its supporters believe it will. To anticipate this future, rather than react to it, appropriate safeguards should be agreed and put in place. Now is not too soon to start. To that end, the authors hope this article will stimulate interesting discussions and constructive debates on the issues it raises, including corporate ethics and privacy in the AmI space; surveillance technologies—from convenience to a false sense of security; the role of horror stories and dark scenarios in ubiquitous computing; and the risks resulting from unwarranted trust. As Thomas Jefferson said, "The price of freedom is eternal vigilance." C

David Wright (david.wright@trilateralresearch.com) is managing partner of Trilateral Research & Consulting LLP, based in London, U.K.

Michael Friedewald (m.friedewald@isi.fraunhofer.de) is a senior scientist and project manager in the Department of Emerging Technologies at the Fraunhofer Institute of Systems and Innovation Research, Karlsruhe, Germany.

Wim Schreurs (wim.schreurs@vub.ac.be) is a researcher at Vrije Universiteit Brussel in Brussels, Belgium.

Michiel Verlinden (michiel.verlinden@gmail.com) is an attorney at the Brussels Bar.

Serge Gutwirth (serge.gutwirth@vub.ac.be) is a professor of law at Vrije Universiteit Brussel in Belgium.

Yves Punie (Yves.Punie@ec.europa.eu) is senior researcher at the Institute for Prospective Technological Studies (IPTS) in Seville, Spain. The IPTS is part of the European Commission's Joint Research Centre (JRC).

Ioannis Maghiros (Ioannis.Maghiros@ec.europa.eu) is principal IST scientific officer at the IPTS.

Elena Vildjiounaite (Elena.Vildjiounaite@vtt.fi) is a researcher at the VTT Technical Research Centre of Finland in Oulu.

Petteri Alahuhta (Petteri.Alahuhta@vtt.fi) is a technology manager in the Mobile Interaction Knowledge Centre of VTT Technical Research Centre of Finland.

DOI: 10.1145/1325555.1325567

[4]Spielberg's 2002 film, *Minority Report*, could be regarded as an example of a cultural safeguard. The film depicts a society, in 2054, embedded with AmI technologies, in which we hear memorable phrases such as "I'm placing you under arrest for the future murder of ...". For a discussion, see D. Wright's, "Alternative futures: AmI scenarios and *Minority Report*," *Futures 40*, (June 2008) *40*, 5.