FUTURE FICTION

2035

(SMART) HOME IS THE EXTENSION OF (DIGITAL) WORK

It is becoming harder and harder to create boundaries between work and home. Smart and connected devices in the home contribute to blurring the lines.

In Norway, companies offer installation of smart sensors and connected devices in the households of their employees. These services openly monitor workers at home, with the aim of helping them to better perform their jobs and prevent work-related diseases.

These connected corporate eyes are plugged into existing connected devices – such as smart speakers, smart fridges or smart vacuum cleaners, or provided as additional connected appliances. The system is especially trending among remote workers, allowing them to track and improve their productivity.

To do so, the corporate devices collect professional data, as well as non-work-related information, helping companies plan new business strategies and organise daily tasks. In short terms, the promise is quite simple: *'tell me how you live, I'll tell you how you'll work better'*.

Workers taking part in these monitoring programs are paid slightly more, as a bonus for welcoming their company into their homes. The willing participants can also use their work data to boost their careers and improve their data-driven CV by showing their dedication through data.

On the back-end, having access to employees' connected houses helps the human resources department adjust the company policies, with more personalised frameworks and schedules. In the balance, giving up a bit of privacy may help the employers anticipate a worker's need for time for and with the kids, but also for leisure and exercise.

At first, the concept of benevolent corporate monitoring targeted employees from service companies who had the chance to work from home. Later, due to its seeming success, the same system started to be applied to non-remote workers, such as construction workers or restaurant workers, with the promise of adapting the workload to their life situations. Now, some workers' unions wonder if the whole system has become a digital way to control workers' lives to better exploit their potential and secure business performance.

Moving to more precarious workers, the corporate monitoring system carries the seductive offer of earning a little extra money through a sort of *'digital labour'*. Those who live on odd jobs are tempted to accept having their data collected by sponsored sensors in their home. These precious digital fragments of life are then sold by the employment agency, while temporary workers earn a fraction of the profit.

At the turn of the 2030s, the practice of blending work and home life is both praised and criticised.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Digital labour or the fragile backbone of Artifical Intelligence (AI)

‘Digital labour’ can be seen as *‘task-based activity that involves fragmenting work so that anyone can do it’*, according to sociologist and researcher Antonio Casilli (Polytechnic Institute of Paris / Télécom Paris). The performance of what we believe to be smart, automated or AI systems are most often based on a human workforce.

Digital labour actors across the world, also called *‘click workers’*, are assigned ungrateful and alienating tasks such as content moderation on platforms and social media or data labelling to train artificial intelligence.

These hidden and poorly paid micro-workers – conveniently presented as an AI – make up a new *‘digital proletariat’*. In 2024, and for the years to come, the development and advancement of key artificial intelligence systems depend on the availability, commitment, and diligence of these independent and precarious micro-workers.

The rise of people analytics

‘People analytics’ encompasses both a trend and a series of tools based on artificial intelligence aimed at better understanding employees and improving business performance. While driven by benevolent ambitions, such as improving well-being at work and promoting work-life balance, they also foreshadow new forms of surveillance at the heart of companies and at home – in remote working environments.

An emblematic example of the people analytics trend is *Hire*, an application developed by *Google* to enhance the recruitment process through AI. The app utilised a disruptive indicator named *ELTV* for *‘Employee Lifetime Value’* to estimate the value a company could expect from each employee. However, the project was abandoned in September 2020.

When employee surveillance alters productivity

The rise of remote working has led to an uptick in surveillance practices within companies. The number of businesses monitoring their employees has doubled since the onset of the COVID-19 pandemic. Some surveillance programs record keystrokes or track computer activity through periodic screenshots, while others monitor phone calls, meetings, and even access employees’ webcams.

However, such measures often prove counterproductive. Research indicates that digital surveillance in the workplace impairs productivity and creativity while increasing stress levels. Simply being aware of being watched can trigger feelings of low self-esteem, anxiety, and depression. Therefore, the implementation of surveillance measures should be approached with caution to avoid detrimental effects on employees’ well-being and overall productivity.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035 THE DATAXATION

The Norwegian State, as well as municipalities, are relying on algorithms and artificial intelligence (AI) to help civil servants operate local and national public services. To run these smart systems, large amounts of reliable data are needed to efficiently anticipate and adjust policies and decisions.

Public taxes have been replaced by a new system called *'dataxation'*, a data-based taxation, requesting citizens to share data about their daily life with the State and local municipalities. Smart homes are a keystone of the dataxation system, with their many sensors taking part in the algorithmic national effort.

In the dataxation system, many domestic devices – such as smart fridges, thermostats or speakers – are constantly collecting and aggregating data on their owners' habits and behaviours, health and consumption. This precious and mostly anonymised stream of information is sent to the public administrations and their partners every week.

The new data-driven tax policy has reduced the fiscal pressure on the households, thus increasing Norwegian people's purchasing power and improving several public services.

However, voices are expressing concerns about invasion of privacy, with the growing volume of personal data requested by the State to fuel its public algorithms. Other people are joking they now have to spend a day off at (smart) home to produce enough data in order to accomplish their fiscal duty.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

The rise of artificial intelligence in the public sector

Western States are increasingly relying on public algorithms and generative artificial intelligence (AI), such as *ChatGPT*, to help civil servants run partly automated public services, with the promise of more efficient and more personalised public services.

In June 2023, the Norwegian Digitalisation Agency (*DigDir*) released new guidance on artificial intelligence for the public sector, open for testing and discussion with stakeholders.

Flawed data leads to biased algorithms

Algorithms and AI need high-quality data to be trained in providing better analysis. In this sense, data are their fuel. However, early studies show that current AIs have been trained with flawed – or even *'poisoned'* – data, creating biases in the smart systems' functioning.

Data poisoning is a tactic used by malicious users to trick a machine-learning system by feeding it misleading data during its training. If trained with flawed or poisoned data, the AI may produce errors or generate wrong analyses.

For example, in early 2024, a *ChatGPT like* chatbot launched by the Austrian Employment Agency was showing sexist biases, refusing to orient unemployed women towards jobs in the IT sector.

Getting paid for your personal data

Several startups are offering users to monetise their personal data. On the digital market, data brokers are collecting and aggregating users' personal data to resell it to other tech companies. They are now challenged by individuals directly getting paid to provide their personal data.

However, a person is inherently weaker than a data brokering specialist in the negotiation and often gets the lowest market price for large parts of their private life.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035 THE CIVIL CYBERDEFENCE

Norway is facing constant cyber aggression from hostile neighbour states and foreign criminal groups. In response, *Forsvaret* (the Norwegian Armed Forces) has decided to strengthen its cyber defence strategy by relying on the population.

Connected households are called to join the civil cybersecurity program to strengthen the digital infrastructure and local communities against cyberattacks. One of the cornerstones of the cyber defence strategy is the *National Botnet Army*, which can be mobilised to retaliate when flexing digital muscles becomes necessary.

In fact, the computing power of every Norwegian smart home device can be integrated into a shadow digital army to perform attacks on the enemy's digital infrastructure.

This strategy relies on *Distributed Denial-of-Service* (DDoS) attacks, which work like online traffic jams caused by flooding a website or online service with too much traffic, making it inaccessible to legitimate users. For the enemy's servers, it is like having so many people trying to enter a store at once that nobody can get in. All of this thanks to networked and weaponised Norwegian smart home technologies!

Concerned with building its digital resilience, the Norwegian State can unexpectedly assess and control connected households to ensure they respect the minimum cybersecurity level determined by the law. As the digital army motto says: '*It's everybody's business to make the country less vulnerable*'. If your connected accommodation has failed a penetration test operated by the authorities, certified advisors may come to your home to provide advice and apply patches to prevent future weaknesses.

In addition, each Norwegian civil cyber defender is following an introductory cyber warfare and cyber defence training during one's military service. Following, every year, a two-day cyber training is a mandatory citizen duty. Revising the basics of cyber defence and getting updated on new threats and practices help protecting and upgrading one's connected household in order to serve the *National Botnet Army* if the dark times of cyberwar come.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

The cyber risks, an invisible yet growing threat

The rise of cyber risks is an invisible yet growing threat globally. According to experts from various panels around the world, cybersecurity risks could potentially trigger the next major global crisis.

Threats such as hacking, identity theft, cyber fraud, and social manipulation have the potential to disrupt democracies, economies, essential services, and international stability. In fact, according to the insurer *AXA* in its *Future Risks 2023* report, cybersecurity risks rank as the second most important systemic risk.

To address these cyber risks effectively, a comprehensive approach is necessary. This includes implementing technical safeguards, providing security awareness training, developing incident response plans, ensuring regulatory compliance, and fostering collaboration with stakeholders across sectors.

By understanding and proactively managing cyber risks, individuals and organisations can better protect themselves against cyber threats and safeguard the integrity, confidentiality, and availability of their digital assets.

Entering the era of state-run cyberattacks and hybrid war

We are entering an era where state-run cyberattacks and hybrid warfare are increasingly common. The Internet and our connected lives have become a new battleground, with countries engaging in digital altercations and critical incidents. Digital tactics, once the domain of criminals, are now part of the modern soldier's toolkit.

Cyberwarfare includes espionage, cyberattacks, sabotage, and disinformation campaigns. Vulnerable smart homes are prime targets for sowing chaos and fear among populations. Authoritarian regimes such as Russia, China, and North Korea have a history of creating disinformation units and training elite hackers. Western countries are also training divisions to defend their national digital infrastructure and launch counterattacks.

For example, *Cyberforsvaret*, the Norwegian Cyber Defence Force, was established to protect Norway's digital infrastructure after cyberattacks. In June 2022, a DDoS attack on the state sector was attributed to a *'criminal pro-Russian group'*. More recently, in July 2024, twelve Norwegian ministries were targeted in a cyberattack, with the perpetrator yet to be identified.

When the *Mirai* botnet uses smart homes to run cyberattacks

One notable example of cyber threats is the Mirai botnet, which has been active since 2016. *Mirai* infects *Internet of Things* (IoT) devices, such as routers, surveillance cameras, or smart fridges, and turns them into remotely controlled bots.

Cybercriminals exploit these infected devices to launch distributed denial-of-service (DDoS) attacks against targeted websites, networks, or services. Mirai operates by scanning the Internet for vulnerable IoT devices, particularly smart gadgets with default or weak login credentials.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035

MEET YOUR SMART HOME THERAPIST

Trained in human psychology and machine learning, *Smart Home Therapists* (SHT) are a new and crucial type of carer. Their role is crucial in (re)building trust and bonds between residents of any age and their smart home when bugs create defiance and distress.

As a growing number of households are welcoming artificial intelligence-driven services, weird situations tend to occur. As a matter of fact, these smart systems come with flaws and biases. They embody the a priori of their makers, reproducing real-world inequalities such as racial or gender bias: people of colour have difficulty being correctly detected by their connected home sensors, disabled people are offered a lower quality of smart services.

Here's where the smart home therapists come into play!
These specialists are the unexpected saviours having emerged from the rise of connected and learning domestic appliances. Their key job roles include:

- Listening and observing, diagnosing and analysing both smart domestic objects and their human owners in order to understand and treat mismatches and incompatibility.
- Recalibrating human behaviour to facilitate interaction between smart objects and their owner, by evaluating the psychological compatibility of the person with the smart home.
- Fixing and adjusting smart appliances to adapt their features to the owner's rituals.
- In more sensitive cases, re-educating smart devices to take disabilities and personal specificities into consideration, and retraining the algorithmic systems when they follow discriminatory stereotypes.

In the early 2030s, one of the most common problems fixed by *smart home therapists* is solving *'data confusion'*, such as in these examples:

— An elderly woman is in conflict with her smart fridge, as the appliance has started operating according to her visiting grandson's dietary profile rather than her own medically prescribed meal plan. The therapist needs to create a new routine to ensure the smart fridge recalibrates to the senior user's profile and lessen the elderly woman's concerns.

— A family is struggling with different preferences for their smart home's lighting and temperature settings. The *SHT* would mediate a discussion to find a compromise that satisfies everyone while optimising the system for efficiency.

— An anxious user becomes frustrated with their smart security system after several false alarms confusing them with an intruder. The *smart home therapist* provides both technical troubleshooting and emotional support to help the distressed user regain confidence in the system.

Attentive, thorough, and even-tempered, the successful *SHT* will work with people to facilitate and improve their relationship with their smart house and their access to personalised domestic products and services. Co-financed by the Norwegian welfare services and the smart home solution providers, therapists ensure that smart appliances are fully delivering on the promises of the personalised domestic services.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Psychological impacts of digital technologies

While technology offers many benefits, it also has potential negative psychological effects. Digital exposure, information overload, and constant connectivity can cause stress, anxiety, and even depression. *Fear of missing out (FOMO)*, social comparison, and exposure to idealised lives are additional stressors, especially for adolescents and young adults.

Smart home technologies often encourage continuous multitasking and divided attention. Constant notifications and alerts can reduce concentration, impair memory, and lead to cognitive overload. Being surrounded by tech at home also raises concerns about data privacy, online surveillance, and data breaches, which can impact mental well-being and fuel distrust.

Addressing these psychological impacts is a challenge for smart home technologists and policymakers. Promoting responsible technology use and fostering healthy offline relationships and activities are crucial for prioritising mental health and well-being.

Virtual services, but real biases

Algorithmic bias and artificial intelligence (AI) bias refer to systematic errors or prejudices in smart systems that can lead to unfair or discriminatory outcomes. These biases can arise from various sources, including the data used to train AI models, the algorithms themselves, or the design and implementation of the systems.

Addressing AI biases requires combining technical, ethical, and regulatory interventions. This may involve ensuring diverse and representative training data, implementing fairness-aware algorithms, conducting thorough bias assessments throughout the development lifecycle, and promoting transparency and accountability in smart AI systems.

Additionally, efforts to increase diversity and inclusion in the coding workforce and engage with affected communities can help mitigate biases and promote the responsible and equitable deployment of AI technologies.

From smart home to techno symbiosis

What if the future of the smart home was the old and persistent myth of the cyborg, a half-human and half-machine being? Smart tech wouldn't be limited to our homes but would be integrated into us. If, for some, the smartphone is already a digital extension of the human; here we are talking about physical hybridisation, the integration of machines into an individual's biology.

Projects like *Neuralink* direct neural interface, led by Elon Musk, *Google* or *Apple* glasses leading to augmented vision, or even connected clothing, suggest future developments that will further advance the digitisation of our daily lives. However, the expected benefits (time, performance, well-being) remain to be confirmed, and the meaning derived from these benefits to be clarified.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035

THE DIGITAL AMNESIA

Many digitally aware households have opted for the implementation of ethical solutions to protect their privacy at home. For example, some *'digital shield'* services are ensuring that data 'leaving' the smart household networked premises has been properly authorised, akin to a virtual guardian.

Recently, a radical tool has gained popularity: a complete solution that automatically erases all collected data within the household every 24 hours, guaranteeing that all data points produced inside the home is erased once it is *'consumed'* or *'used'* by a digital domestic service.

Several services have positioned themselves in this niche and offer management solutions for this practice of selective data clearing.

Some users prefer to opt for a manual mode. This is the case for a growing number of Norwegian people practising *'The Digital Amnesia'*, a trendy ritual among the upper middle-class. Before going to sleep, the members of the connected household gather to review, in complete confidentiality, the data generated on that day within the home. Each person decides which data concerning them can be kept in memory and which should be erased.

The *Digital Amnesia* movement advocates this ritual as a way to control and clean up smart household members' activity traces to present a good image to each other. A collective habit to recall the joyful highlights of the day, but also to forget those moments one does not want to resurface.

Indeed, there is an emerging and troubling practice within Norwegian families and couples: the use of smart home devices for everyday micro-blackmail. Thanks to continuous recording features, it has never been easier to replay or resample what was said or done at home, so that these moments of life serve as *'evidence'* when needed, namely during family or marital disputes.

Some detractors claim the *Digital Amnesia* ritual is just a sweet placebo for privacy, questioning if an illusion of data control is better than no control at all.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

A well-established privacy paradox

The *privacy paradox*, a well-known phenomenon, underscores the apparent disparity between individuals' concerns regarding privacy and their actual online behaviour. Despite expressing apprehension about privacy breaches, particularly marked by extensive data collection, many people persist in sharing personal information with connected devices and on online services without much consideration for the consequences.

One driving force behind this paradox is the prioritisation of convenience over privacy. Individuals often willingly share personal data to access online services or features, without fully contemplating the long-term ramifications. Additionally, there's a significant level of trust in institutions and platforms handling personal data, despite numerous instances of data breaches and misuse.

Another factor is that privacy policies and terms of service agreements often are lengthy, complex, and filled with legal jargon. This can make it difficult for individuals to fully understand the extent to which their data is being collected, used, and shared. Social norms and peer pressure also influence online behaviour, with individuals feeling compelled to share personal information to fit in or avoid missing out on social connections and opportunities.

The European Union law provides a right to erasure, commonly known as the right to be forgotten, empowering individuals to request the deletion or removal of their personal data from databases. However, the process can be complex, leading to the emergence of paid automated data deletion services, aiding users in withdrawing their personal information from data brokers selling it.

Neuroprivacy: is cognitive liberty in danger?

In 2024, *Nesta*, the *'UK's innovation agency for social good'*, is sounding the alarm as scientists from the National University of Singapore and the Chinese University of Hong Kong demonstrate the ability to reconstruct basic video content from viewers' brain activity. As a *'market for mind reading'* may emerge in a less advanced form, this new field of data collection raises questions about the necessity to safeguard not only our private life, but also our cognitive liberty in the near future.

In a near future, we may need guidelines for *'neuroprivacy'*, a legal protection of an individual's neural data, which is information derived from the brain's activity, such as thoughts, emotions, and cognitive processes.

Our connected lives already exert an impact on cognitive capabilities, with digital information saturation and fleeting attention becoming valuable commodities for advertisers. *Neuroprivacy* thus extends beyond safeguarding privacy to protecting mental health: will it still be possible to forget and be forgotten? How can information in our mind not be turned into exploitable data? Is our erased data still stored somewhere in our brain? What will it be like to think freely at home?

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035

POLYPROFILES

Digital identities are reflecting the growing need to assert and respect one's gender and cultural identity. Norway is a pioneer in this matter. In the fjord country, no one is a linear steam. Each household member is invited to assume multiple identities by choosing what the user wants to show or hide; especially if this person feels like they are many. The digital identity within the connected household is coherent with a person's path of life and reflections on who she/he is, or they (hen) are. Smart services no longer frame anyone in a category they feel they do not belong to.

On a daily basis, the new *polyprofile* system makes it very easy for a user to switch between profiles, so the smart house adapts to how/who the person feels they are today. New services or specific pronouns are then set in place, following respectful guidelines regarding gender and cultural identities. It has become very common in Norwegian smart homes to hear *'Hey house, today please data-me as A rather than B'*; *'data-me as...'* being a new trendy idiom.

Some digital identities might be logged as strong–'I deeply see myself as this'–while other identities qualified as emergent– *'There might be some nuances, I'm feeling I may become this person, please anticipate and let me try out my everyday life as such'*, as in a mundane rehearsal of new identity. It is equally simple to reverse identity without constraint, building trust between the smart house system and its owners.

A personalised privacy dashboard lets users tell the house how they want to be *'data-ified'* for each of their profiles: what personal data should be collected, how detailed the data should be on this aspect of one's life, what data should never be collected, and what data other household members can consult.

On a more surprising note, the *polyprofile* system is especially favoured by the ageing population. While the elderly people are losing autonomy, carers use the *polyprofile* system as a rich digital memory. It is used to save and secure individual preferences, allowing for switching between profiles, for example, depending on how one's neurodegenerative diseases evolve, and then helping the older person to remember.

When one's time has passed, those polyprofiles become a digital legacy, defining how to be commemorated. The smart home shares the deceased's selected digital profiles and data as a *'message from beyond the grave'* to inspire next of kin in their eulogy or to clarify a bequest. For its promoters, even in death, the *polyprofiles* system combines respect for privacy and identities.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Embracing gender diversity with a shift towards inclusivity

Over the past decade, there has been a shift away from a binary understanding of gender, with scientific evidence challenging outdated views. This movement has led to growing recognition of androgynous and non-binary identities, though progress is slow. Individuals who don't conform to traditional gender norms are asserting their identities and demanding recognition.

Moreover, there is a palpable increase in tolerance towards a broader spectrum of gender identities. Initiatives like *Trans Visibility Month* aim to raise awareness, challenge stereotypes, and promote acceptance, fostering a more inclusive society.

Media, including fictional works such as series and films, as well as social media platforms, play a crucial role in shedding light on gender-related issues and raising collective awareness. Meanwhile, organisations like *AnitaB* advocate for understanding gender discrimination, especially in tech, emphasising the need for diversity in developing inclusive smart products.

Multiple profiles are trending

Managing multiple profiles online is becoming as popular as private browsing to protect one's privacy. On social media, many individuals maintain separate accounts, one for public display and another for friends and family.

Noticing this trend, major tech players and platforms, such as *Google Chrome* and *Meta (Facebook)* allow users to have multiple personal profiles on their platforms since 2023. This feature enables users to switch between personal and professional profiles freely, and selectively share feed posts with *'close friends'* only, such as on *Instagram*.

The White Box

The *White Box* – designed by the *Automato* studio – is a (fictional) concept of a *'smart-but-transparent'* interface for home environment monitoring. It allows users to adjust home parameters through a simple and familiar switchboard. Household members can then select which data is collected by the device – location, environment, biometric data, market data, etc., and even turn on and off stranger parameters such as *'if you want the home to behave in a selfish way or do what's best for the environment and others'*.

In a way, the White Box carries a vision of a *'smarter intelligence'*, a proposal of an evolved back-end empowering people to better understand and control their connected home. Although not intended for sale, the system looks real enough to communicate and question new needs and challenges that *'smartness'* and connectivity bring to our (smart) housing.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2030

REPAIRING TOMORROW

It is the fifth edition of the *National Digital Fixing Day* in Norway, celebrating the new repair culture that has taken hold of the country.

It all started with a consumer's rebellion against the so-called *'big tech greed'*. As the market of digitally connected products began to show some signs of slowing down, smart product manufacturers relied even more on planned obsolescence and subscription models to maintain profits and keep shareholders happy. The strategy initially targeted smart home owners or aspiring buyers by designing new products for households that offered few innovations but had a limited lifespan, all to drive new sales.

Repair quickly emerged as the key strategy for users and consumers to counter these underhanded tactics by smart home solution manufacturers and digital service providers; nobody wanted to feel trapped at home, with basic domestic services that could be discontinued overnight when a new device was marketed, or the subscription plan had changed.

The repair culture in Norway has since flourished, empowering households to maintain and fix their connected homes independently. Local universities offer repair courses and digital literacy classes, while community-managed *repair cafés* provide workshops, tools, and assistance. Matchmaking systems, inspired by dating apps, quickly connect users with nearby repair volunteers, and repair parties are becoming popular social events.

The state has also played an important role in subsidising the shift towards a digital repair culture, with a dual opportunity in mind:

> Equipping people with repair skills could reduce Norway's dependency on foreign smart product manufacturers in an unstable world.

> Repair culture could incentivise Norwegian tech companies to offer new repair options to attract new consumers across Europe, such as providing tools and technical documentation for free, especially for discontinued smart products.

Numerous digital jobs, from marketing to engineering, were destroyed along with the planned obsolescence, but it also created many new meaningful activities in the growing repair economy.

This digital repair culture has overtaken consumerist habits, making the disposal and replacement of smart home products a thing of the past. Repairing is now part of daily life, making smart homes more sustainable, economical, and user-friendly.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

The historic planned obsolescence meets the new subscription fatigue

Planned obsolescence is now well documented, with some manufacturers intentionally designing smart products to become obsolete to drive new sales.

Meanwhile, online platforms and connected devices have adopted subscription-based models, leading to *'subscription fatigue'* — a growing frustration as consumers manage increasing numbers of services. As more businesses adopt these models, users juggle multiple recurring payments for various services, including for their smart homes.

This combination of planned obsolescence and subscription fatigue pushes consumers to seek sustainable, cost-effective alternatives. These include durable, repairable products and services offering clear, long-term value without ongoing costs, fuelling movements like *'Right to Repair'* and the rise of a digital repair culture.

Enforcing a *Right to Repair*

Globally, there is rising pressure on governments to legislate the *Right to Repair*, giving consumers the legal right to fix their devices. This movement is especially strong in Europe, where the 2024 directive on repair of goods requires manufacturers to offer affordable repairs and inform consumers of their rights.

The *Right to Repair Movement* also advocates making repair culture affordable and accessible to all. European countries must implement measures such as repair vouchers, information campaigns, repair courses, and support for community repair spaces.

As consumers grow more eco-conscious and budgets tighten, the *Right to Repair* is key to supporting the circular economy, which prioritises reusing, refurbishing, and recycling.

Repair cafés and pop-up workshops

The increasing popularity of repair cafés and local workshops is a grassroots signal that the (digital) repair culture is becoming more embedded in communities. These spaces not only provide tools and expertise but also foster a sense of community and shared responsibility.

Repair cafés and local workshops have their roots in the well-established *DIY* (*Do-It-Yourself*) and *Maker Movements*, seeking to empower individuals to take on repair tasks themselves. Online communities, open-source designs, and access to affordable tools have democratised repair, making it more accessible to a wider audience, even those with minimal prior knowledge.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035 DESMARTIFICATION

A decade ago, it would have been unimaginable, but smart technologies have lost their appeal. The global cultural shift known as of *'desmartification'* has affected Norway and many Western countries. To understand the growing disaffection for connected devices, particularly smart home solutions, consider two key statistics from the early 2030s:

— 80% of Norwegians experienced a cyberattack or digital crime in the past six months, including a nationwide ransomware attack that demanded a ransom to restore access.

— 90% of users are concerned about digital anxiety and stress, such as fear of missing out and constant notifications, affecting their mental health.

Data breaches, corporate surveillance, and intrusive monitoring further deepened disillusionment. Generative artificial intelligence (AI) like *ChatGPT*, once hailed as revolutionary, proved to be a costly gimmick with little practical value. As startups collapsed and investors withdrew, users were left with AI-driven smart appliances and homes filled with *'bricked'* devices, prompting many to reconsider life without smart tech.

Inspired by the concept of *'Dry January'*, a particular *desmartification* movement originated in Norway, inviting users to live a week, then a month, without smart technology. This slow but steady shift led people to *'desmartify'* parts of their lives and homes, either temporarily or permanently.

Over time, our digital lives were transformed. *'Demarketing'* on social media gained traction, both driven by *hacktivists* (part hacker, part activists) exposing flaws in smart products, and influencers now encourage thoughtful consumption of smart gadgets.

Vintage devices and *retroware* – software or hardware emulating or recreating older technologies – are now becoming the new *'sexy'*, despite security concerns due to outdated software and lacking updates. Going back to analogue solutions and non-connected devices lets users finding joy and taking pleasure in the limits of these *not-that-smart* systems.

Collective households enforce *'no smart tech'* rules or offer shared local data storage to reduce reliance on tech companies.

However, the biggest challenge of *desmartification* remains: in a still connected Norway, abandoning smartphones in favour of *'dumbphones'* is difficult, though these are seeing an unexpected revival. Rumours suggest the government may soon announce a nationwide *'digital rollback programme'* to offer alternatives to smartphones for everyday tasks.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Digital minimalism and tech detox

A growing movement towards digital minimalism encourages individuals to reduce their reliance on digital devices and online platforms, reflecting a desire for a simpler, more intentional way of living. At the same time, the rising popularity of *digital detox retreats*, where participants disconnect from technology entirely, hints at a backlash against constant connectivity.

This trend is further driven by increasing awareness of the negative impacts on mental health of perpetual online engagement, such as anxiety, depression, and attention disorders. As a result, some are opting for *'dumbphones'* (such as clamshell phones) or minimalist devices with limited functionality to reduce distractions and promote mental well-being.

The *Tech Backlash* and ongoing scepticism

The public sentiment is increasingly wary of large tech companies and their influence, fuelling a desire for alternatives less dependent on corporate-controlled platforms.

This scepticism is accompanied by legislative actions targeting big tech, including antitrust regulations and restrictions on data collection, as well as grassroots movements advocating for open-source or non-digital alternatives.

Additionally, there is a growing interest in retro technology, such as retro gaming or even simple phones, which celebrates pre-digital or less digital lifestyles, as seen in the *Slow Movement*; advocating for slowing down life's pace, as well as for deliberate, mindful practices in areas such as food, travel, and living to foster greater quality, sustainability, and well-being.

The *low-tech*, a meaningful approach of innovation

Over the years, the plural *low-tech* movements advocate for a more responsible and meaningful approach to innovation, challenging the trend of over-technologisation in modern life. These movements have in common to emphasise simplicity, sustainability, and the preservation of traditional knowledge, arguing that not every problem requires a high-tech solution.

Instead of constantly pursuing the newest and most advanced technologies, the low-tech philosophy encourages the reasonable use of durable, repairable, and resource-efficient technologies and designs that meet human needs without unnecessary complexity or undesirable side effects.

By focusing on the essentials and avoiding the excesses of smart products, this approach seeks to create a more sustainable and equitable future, where technology serves humanity without overwhelming or detracting from the quality of life.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035

STUCK IN THE NORNET

The Internet has fragmented into separate regions, replacing the once-global network that connected all countries. This is the era of the *Splinternet* – the split Internet – where the network of information and smart services has been divided. At the heart of this shift, *geofencing* technologies have created virtual borders around specific areas, blocking people outside these zones from accessing digital services or smart devices.

Norway, along with many other European countries, has been affected by this nationalist turn of the Internet. It has been cut off from other regional networks, such as the Russian *RosNet*, the Sino-African *Prosperity Net*, and even the Great American-Britain Net. To thrive in this disconnected world, Scandinavian states and related tech companies have set their differences aside and collaborated to build the *Nordic Network* (or *NorNet*).

NorNet has become a regional sovereign network, crucial during recurring *'Internet blackouts'*. Access to Chinese and US-based smart tech services is now unreliable, dependent on fluctuating diplomatic relations. Many Nordic users are shocked to realise that their smart homes, though located in Lillhammer or Bergen, rely on servers in Silicon Valley, Singapore, or Hangzhou. Overnight, your beloved vacuum cleaner could be rendered inoperative due to an unrelated disagreement between Oslo and Beijing on how to account for carbon emissions.

Across the country, many Norwegians find themselves stuck simultaneously with and in the *NorNet*, dealing with very limited but always active smart home appliances, provided by local startups and telecom companies. Given fewer available options, Norwegian users have begun to reconsider what is truly necessary to enjoy a good digital life. Some are scaling back their smart tech to ensure reliability, while more adventurous users track geopolitical trends to predict whether their smart devices will function properly.

Hiring a *cyber-smuggler* or befriending a *VPN-Chief* – a virtuoso in managing virtual private networks, a system allowing you to hide your connection location– has become quite common to get access to foreign cloud-based or smart solutions, especially from the US.

After a few years of *Splinternet* limiting global content and services, Norwegian users have begun to find tailored smart home services optimised for Scandinavian needs. These services comply with *NorNet* regulations, offering enhanced privacy protections but also signifying increased government surveillance.

The *NorNet*, affectionately dubbed *Our MiniNet*, has proven resilient, ensuring stable and essential smart services during geopolitical crises, such as the China-Taiwan war of 2037, which threatened key components for digital technologies.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

The regionalisation of digital platforms and content

The Internet, originally envisioned as a global network, is increasingly shaped by regional influences. Countries and regions are promoting or developing their own social media platforms, search engines, and online services tailored to local needs and regulations. For example, China's *WeChat* and Russia's *VKontakte* dominate their respective markets, while global platforms like *Facebook* or *Google* face restrictions or must adapt to operate in these regions.

Likewise, content available in one country might be censored or entirely inaccessible in another due to differing laws and cultural norms. This trend could lead to an Internet experience that varies significantly depending on the user's location, diminishing the once universal nature of online access and interaction.

The plausibility of a near-future *Splinternet* is a topic of discussion among experts, as state practices , such as government-initiated *Internet blackouts* in India, challenge the notion of a unified and open internet.

An expansion of digital sovereignty and national control

Governments are increasingly asserting control over the Internet within their borders, often citing reasons such as national security, cultural preservation, or economic independence. This is manifested through laws that govern data localisation (requiring data to be stored within national boundaries), the creation of national firewalls (such as China's *Great Firewall*), and the development of state-controlled digital currencies (for instance, the digital yuan in China).

These actions are part of a broader trend towards digital sovereignty, where nations seek to control the flow of information and the operations of global tech companies within their borders. The result could be a more segmented Internet, where users experience different digital realities depending on their country's policies and governance structures.

Diverging technological and cybersecurity standards

As countries and regions develop their own technological standards, the global interoperability of devices, networks, and services is increasingly at risk. For instance, the rollout of 5G technology has seen different regions adopting varying standards and regulations, influenced by both technical considerations and geopolitical tensions.

Similarly, cybersecurity practices are diverging, with some countries imposing stringent data protection laws, while others focus on surveillance and control.

These differences may lead to a situation where digital products and services are not universally compatible, further isolating regional Internet ecosystems. The fragmentation in standards could hinder international cooperation, limit global innovation, and create barriers to the seamless global Internet experience that many users have come to expect.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2030

WELCOME TO THE CABIN, YOUR NEW DIGITAL SAFE PLACE

Hacker attacks on the *Internet of Things* and smart home devices, orchestrated by adversarial foreign nations or cybercriminals, have become a global problem. Many people fear that crucial functions within their home can be targeted from anywhere in the world. In response, building self-sufficient smart homes has become essential.

In this context, family cabins in the Norwegian wilderness are often seen as sources of inspiration, embodying simplicity and resilience. These cabins have evolved into laboratory-like spaces for experimenting with new ways of thinking and living in self-sufficient and resilient smart housing. Three major cabin models can be observed across the country, each offering a unique approach to strengthening smart home technology:

- The first and main model involves using the cabin as a playground to test new smart home technologies before deploying them at home. The goal is to trial innovative smart living solutions while minimising risks. Following this trend, several manufacturers have begun supplying disconnected smart home products specifically for cabin use.

  These products feature powerful built-in computers that can control lighting and heating based on usage patterns detected by sensors in the house. Robot vacuum cleaners function without an Internet connection. Other domestic devices process data locally and use built-in artificial intelligence. Although these devices are more expensive and offer fewer features than their cloud-connected counterparts, they are far more secure.

- The second model is the *'Retreat'*: users spend time at their cabin to reflect on whether they are ready to (re)connect parts of their home. Ethical smart tech manufacturers offer meditation programmes during these retreats, helping users assess the benefits and risks of connectivity.

- The third model designates cabins as *'smart tech free zones'*. These offline spaces serve as safe havens during cyberattacks or periods of digital anxiety.

In Oslo, Trondheim, and Lillehammer, the lessons learned from these cabin experiments are reshaping the outdated concept of the smart city. Smartness is being redefined with more robust technology and thoughtful applications. Once seen as a nostalgic relic, the Norwegian cabin has become a vital asset in facing the cyber risks of the 21st century.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Welcome to the era of cybersecurity threats!

The increasing frequency and severity of cyberattacks, particularly on smart infrastructure and devices, have exposed the vulnerabilities of highly connected systems, leading to a preference for more secure, less connected alternatives. Experts predict that cyber risks may soon be excluded from standard insurance coverage due to the potentially massive losses that cyberattacks can cause, which insurers may struggle to bear.

Home insurance coverage is still at a crossroads: equipping households with smart devices could reduce insurance costs, as the collected data can help in adjusting a personalised protection plan and sensors can help prevent fires or water leaks. However, it could also drive costs up due to the increased risk of cyberattacks compromising the connected home.

Over the next decade, this could result in higher premiums and a redefinition of what constitutes a cyber risk, making users more hesitant to adopt smart solutions.

Digital technology doesn’t necessarily mean connected technology

In recent years, technology that stores and processes data locally in the devices rather than in cloud services has become more widespread. Some neighbourhoods and districts are testing out local wireless networks that are separate from global networks. This provides less access to the most advanced features, but it protects users and their devices from outside attacks.

A weak signal of this controlled disconnection could lie in the looming interest in *low-tech* security measures and the adoption of *‘air-gapped’* systems that are isolated from the Internet.

The ongoing struggle of ethical design

Across Europe, ethical design collectives advocate for digital technologies that prioritise users’ well-being, privacy, and fairness. They challenge exploitative practices like *surveillance capitalism*, where companies profit from collecting and monetising personal data without explicit consent.

These movements promote products and services that are transparent, respect user data, and are ethically designed. By promoting a more reflexive use of digital technologies–where users and creators alike are more aware of the implications of their digital interactions–these movements can strengthen cybersecurity.

As ethical design becomes more prevalent within the innovation labs of smart tech manufacturers, systems are built with stronger privacy protections, reducing both vulnerabilities and inviting new fairer way to consider user data.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2030

RENTING UNDER SURVEILLANCE

The relationship between landlords and tenants has been transformed by the pervasive use of smart technology in rental properties. It began as a means to enhance security and efficiency, such as ensuring faster maintenance when specific repair needs were detected. It has now evolved into a system of constant surveillance, fundamentally altering the dynamics of renting.

Landlords, motivated by a mix of paranoia and the desire to protect their investments, have started outfitting their properties with an array of smart devices. Connected doorbells, smart thermostats, and energy meters become standard features in rental units.

Initially marketed as conveniences, these devices reveal their true purpose: monitoring tenants' every move. Data on energy consumption, room occupancy, and even visitors to the home – everything is streamed directly to landlords, allowing them to enforce rules and maintain control with unprecedented precision.

For tenants, this constant surveillance feels intrusive, eroding the privacy and autonomy that a home should provide. The rental agreement has shifted from a simple exchange of money for shelter to one that includes ongoing surveillance, often without explicit consent. These smart devices, often impossible to disable, turn homes into monitored zones where every action can be scrutinised.

Turning up the heat on a cold night can result in a stern warning about excessive energy use. Visitors arriving late at night might trigger a notification to the landlord, questioning the tenant's adherence to agreed-upon rules. Even the simplest act, such as cooking dinner at an unconventional hour, is prone to invite scrutiny.

As these practices become widespread in cities like Oslo and Bergen, properties without such surveillance are increasingly rare and expensive. In this paranoid real estate market, the ethical implications of smart technology comes into sharp focus. The balance of power is, more than ever, unequal: if a tenant agrees to the landlord's smart monitoring, it may increase their chances of being selected for the desired accommodation.

Recently, a new trend has emerged among connected landlords: offering tenants a rent reduction in exchange for adopting an artificial intelligence-driven *smart Valet*. This system checks the '*integrity*' of the accommodation each week and provides advice on how to keep the home clean and functional, based on data collected by various sensors and devices.

For those living under this surveillance, the rise of domestic monitoring serves as a cautionary tale, questioning whether the comforts of modern smart technology are worth the cost to privacy and autonomy.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

When Surveillance Capitalism fuels the rental markets

The growing use of data collection and monitoring in various aspects of life, particularly by tech companies, is being mirrored in domestic spaces. Landlords and property managers are beginning to see value in the data generated by tenants, potentially using it for purposes beyond just maintaining the property.

It relates to the concept of *Surveillance Capitalism*, a new economic system where companies collect vast amounts of personal data, often without individuals' full knowledge or consent, and then use this data to predict and influence behaviours. This data is primarily gathered through digital platforms and services, such as social media, search engines, and smart devices.

The introduction of surveillance technologies exacerbates the power imbalance in rental markets, as tenants may feel they have little choice but to accept these conditions if they want a place to live.

The expanding integration of artificial intelligence in property management

The digital market sees new instances where artificial intelligence (AI) is being used to monitor and manage properties, from predicting maintenance needs to monitoring energy usage. The democratisation of this smart technology for landlords and property owners could lead to more comprehensive surveillance systems that go beyond basic security.

At the same time, some insurance companies are beginning to offer discounts or benefits to homeowners who use smart surveillance systems, including AI in some solutions, subtly encouraging their adoption. However, this would cause further entrenchment of surveillance practices, potentially making them a de facto requirement for renters.

Tricking smart surveillance systems as a playful activity

A new trend in digital culture involves playful resistance against smart surveillance, where individuals creatively deceive or disrupt data collection technologies. Art projects like *Uninvited Guests* (from *Superflux*) and *Unfit-Bits* (from *Tega Brain*) encourage using ordinary objects or exaggerated behaviours to confuse smart devices and algorithm-driven homes.

This trend reflects growing awareness and critique of pervasive surveillance, as well as a desire to reclaim control over personal privacy in a data-driven world. These actions challenge the accuracy of surveillance systems and underscore the tension between technological convenience and privacy rights.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!

FUTURE FICTION

2035

DEALING WITH THE SMART GREEN QUOTA

It has been seven years since the Norwegian government, driven by a commitment to sustainability, introduced the *Smart Green Quota*, a policy designed to reduce the environmental impact of digital life. Each household is now assigned a limited quota, a cap on the number of smart devices they can own and operate during the next decade. The quota is calculated based on the green footprint of each device, factoring in energy consumption, production emissions, and resource usage.

Citizens can choose their devices carefully, switching them out as needed, but they can never exceed their allocated quota without facing stiff penalties. Individual quotas may evolve according to the surprises of life; however, exceeding the quota still results in fines or future restrictions, compelling citizens to carefully manage their digital assets.

The *Smart Green Quota* policy has transformed daily life, forcing families to make tough decisions about which smart devices are truly essential. Smartphones, once frequently upgraded, are now kept for years to avoid high footprint costs. The energy efficiency of appliances is scrutinised, with many opting for older or analogue alternatives to conserve their quota.

A culture of digital frugality has emerged, with households closely monitoring energy use and receiving reports that track device usage against their quota. Communities have developed creative strategies to cope, such as sharing devices and modifying existing tech to reduce energy consumption.

However, the quota has also highlighted growing inequality. Wealthier citizens, able to purchase the latest, most efficient devices, find it easier to stay within their limits. In contrast, lower-income households, often relying on older, less efficient tech, struggled to comply with the restrictions. This digital divide deepens, tying access to advanced technology to one's ability to pay for a smaller environmental footprint.

The *Smart Green Quota* has sparked ethical debates, with some seeing it as government overreach. Concerns about privacy and state control have been raised, as monitoring device usage and energy consumption feels intrusive. Critics argue that enforcing the quota through surveillance is both costly and invasive.

Despite these challenges, the *Smart Green Quota* has had a profound impact on Norwegian society, encouraging a culture of mindfulness where every digital choice matters. People have become more aware of the environmental costs of their devices, leading to a shift towards more sustainable consumer behaviour.

As the world watches Norway's experiment, it is clear that the *Smart Green Quota* is not just an environmental policy, but a test of society's ability to adapt to a sustainable future.

How would your daily life look in this future?

What has changed? How would you adapt to or resist this situation?

After answering this question, turn the page.

TODAY

SOME SIGNALS MAKING THIS A POSSIBLE FUTURE

Environmental sustainability may need technology regulation

The increasing awareness of the environmental impact of digital technology is driving regulatory efforts to reduce the carbon footprint of devices and data usage. Governments are starting to introduce sustainability measures, such as energy efficiency standards and potential carbon quotas for digital life, aimed at curbing the environmental effects of technology.

Initiatives like carbon footprint quotas for households and programs promoting device longevity suggest a future where sustainability becomes a central criterion both in consumer choices and in the regulation of digital life by legislators. In the near future, this could lead to policies that invite users to reduce the number of smart devices they own based on these products' environmental impact, similar to the *Smart Green Quota* from the fiction.

Digital inequality challenges our consumer behaviour

The digital divide remains a significant issue, with wealthier individuals more capable of affording the latest, most efficient devices, thus more easily staying within the limits of environmental regulations.

Simultaneously, there is a growing movement towards minimalism and mindful consumption, where people are more aware of the environmental cost of their tech choices and opt for fewer, longer-lasting devices. As in the case of energy transition, without inclusive safeguards, legislation on the green footprint of smart home solutions may eventually worsen the digital divide.

The unexpected green footprint of smart technologies

The green footprint of smart technologies refers to the overall environmental impact of these devices, from the moment they are made to the end of their life. This includes the energy consumed in manufacturing, the extraction and processing of raw materials like metals, plastics, and rare-earth elements, and the electricity needed to power them during use. As the number of smart devices–such as thermostats, speakers, and appliances–grows, so does their collective environmental impact.

When discarded, smart devices add to the rising problem of electronic waste (e-waste), which is difficult to recycle and often ends up in landfills, releasing toxins into the environment. To reduce the green footprint of smart tech, it's essential to focus on energy-efficient design, mindful consumption, and improved recycling practices, balancing the benefits of smart technology with its environmental costs.

What can you do today to prepare yourself and your household for this future?

After answering this question, explore another future fiction!