



laetus in praesens

Alternative view of segmented documents via Kairos

23 February 2015 | Draft

Naive Acquisition of Dual-use Surveillance Technology

Progressive market-driven transformation of personal appliances into spyware?

-- / --

Introduction

[Vulnerabilities of domestic technology -- notably to hacking](#)

[News reports -- critical and otherwise](#)

[News reports -- apologetic and otherwise](#)

[Disabling "smart features" and questionable "loss of settings"](#)

[Dual purpose and Doublespeak: features vs exploitation](#)

[Legality of subsequent use of recorded information](#)

[Smartening TVs and dumbing down content?](#)

[References](#)

Introduction

February 2015 has been witness to worldwide news coverage of the manner in which new "Smart TVs" were designed to listen to, if not visually record, those watching them. The major issue of concern was how the information acquired in this way was used, by whom, and with what constraints. The point variously made is that many forms of "smart technology" are now enabled in this way with questionable implications for the user. The case of the TV is therefore to be usefully considered as symptomatic of a wider challenge for users. The controversy offers insights into what might be appropriately termed "domestic espionage" or espionage with user complicity - reminiscent of issues famously raised by George Orwell in *Nineteen Eighty-Four* (1949).

Coincidentally it so happens that the author of this document purchased such a TV a month previously in order to replace a set which had been operating for 20 years -- so as to benefit from a wider range of program channels and the extra features associated with newer technology. This note reflects the consequences of immediately raising the reported issues with the vendor from which it had been purchased.

The personal experience gives focus to the concern that installation of a device, enabled in this way, transforms an environment into one which bears a curious resemblance to the interrogation room of a security service -- observing those present through a one-way window. In cultivating a [culture of fear](#), creating this impression may be the intention of some parties.

The most recent concerns about the Samsung Smart TV have been evoked over the same period as the [White House Summit on Cybersecurity and Consumer Protection](#), it is therefore appropriate to recall the techno-optimism which characterizes Silicon Valley and its followers. A valuable question had been raised -- in the period when the possibility of hacking the Smart TV had already been reported (Charles Kenny and Justin Sandefur, [Can Silicon Valley Save the World? Foreign Policy](#), 24 June 2013). It has been recognized that "defeating global poverty" was the latest start-up trend -- with the question *But is there really an app for that?* This article has evoked various responses (Stefaan Verhulst, [Can Silicon Valley Save the World? GovLab Digest](#), 24 June 2013; Leigh Buchanan, [Will Silicon Valley Save the World? No, But Here's What Will, Inc Magazine](#), 29 July 2013; Ned Breslin, [Silicon Valley Won't Save the World, but..., Stanford Social Innovation Review](#), 2 July 2013; David Gura, [Why Silicon Valley can't end world poverty, Marketplace](#), 27 June 2013).

There is therefore considerable irony to the current preoccupation with cybersecurity to protect any "homeland" -- with the aid of dual-purpose Silicon Valley high-tech effectively designed to invade the home. Is the purpose indeed to increase the sense of threat and insecurity in the expectation that people will turn to authority?

Vulnerabilities of domestic technology -- notably to hacking

Especially intriguing in the recent news reports is the concentrated focus on the "listening" capacity of Smart TVs. Almost nothing is said about the ability of a superior model also to offer visual recording features to enable other interactive communication processes, video conferencing, and the like.

Hacking: A research report on the possibilities of hacking a Samsung TV was presented at the [Black Hat cybersecurity conference](#) (Las Vegas, 2013), By [Aaron Grattafiori](#) (*The Outer Limits: hacking a Smart TV*, iSEC Partners, October 2013), it is widely cited (Eduard Kovacs, *Samsung Smart TVs Can Be Hijacked, Researchers Warn*, *Softpedia*, 5 August 2013; Erica Fink and Laurie Segall (*Your TV might be watching you*, *CNN Money*, 1 August 2013).

The report compares the number of models and features of Samsung (69) with those of others, potentially characterized by similar issues: LG (49), Sharp (23), Panasonic (18), VIZIO (8), Philips (16), Toshiba (12), Sony (10), Lenovo. It cites an earlier study (Seunglin Lee: *Hacking, surveilling, and deceiving victims on Smart TV*, Korea University, 2013). The presentation of that work in Las Vegas is also summarized by Stilgherrian (*Smart TVs are dumb, and so are we*, *ZDNet*, October 2013). He remarks that SeungJin Lee can turn a smart TV into a surveillance and disinformation machine, thanks to the vendor's slack security coding.

Vulnerabilities: Such reports reveal an astounding range of poorly recognized vulnerabilities which place the user at risk of exploitation.

Smart TV sales had reached 67 million in 2012. The vulnerabilities had been reported to Samsung in early January 2013 and resulted in software upgrades by Samsung.

- Leo Kelion (*Samsung's smart TVs fail to encrypt voice commands*, *BBC News Technology*, 18 February 2015)
- *Samsung investigates why its TVs put ads in others' apps*, *BBC News Technology*, 11 February 2015
- *Not just listening: Samsung TVs send out unsafe unencrypted' data*, *Guerilla Media Network*, 19 February 2015

The current issue is seen as part of a general trend (*Smart Devices: is privacy loss inevitable?* *BBC News Technology*, 10 February 2015; Alex Hern, *6 Ways Your Tech Is Spying on You: -- and how you can fight back*, *The Guardian*, 10 February 2015). Failing an appropriate response, the claim is made that the situation is going to get worse. Curiously, with respect to the Samsung Smart TV, the vendor to which protest was made had only just been made aware of the problem and the controversy it had aroused.

As noted in the succinct *CNN Money* report (*Your TV might be watching you*, 1 August 2013):

The flaws in Samsung Smart TVs, of which some have reportedly been patched, enabled hackers to remotely turn on the TVs' built-in cameras without leaving any trace of it on the screen. While watching TV, a hacker anywhere around the world could effectively be watching the viewer. Hackers also could have easily rerouted an unsuspecting user to a malicious website to steal bank account information. Samsung quickly fixed that problem after security researchers at iSEC Partners informed the company about the bugs -- sending a software update to all affected TVs. These issues highlight a larger problem of devices that connect to the Internet but have virtually no adequate security. Security cameras, lights, heating control systems and even door locks and windows are now increasingly delivered with features that allow users to control them remotely. Without proper security controls, there is little to stop hackers from invading the privacy of users, stealing personal information or spying on people.

News reports -- critical and otherwise

Privacy policy: Subsequent to the early reports, the flurry of recent news coverage was triggered by a report regarding the legal small print associated with the Samsung Smart TV (*Watch Your Mouth: Your Samsung SmartTV Is Spying on You, Basically*, *The Daily Beast*, 5 February 2015):

A single sentence buried in a dense "privacy policy" for Samsung's Internet-connected SmartTV advises users that its nifty voice command feature might capture more than just your request to play the latest episode of *Downton Abbey*.

The Daily Beast noted a sentence in Samsung's privacy policy and framed it as a smoking gun. "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

Based on previous [customer references](#), that "third party" converting speech to text is Nuance. Nuance provides voice recognition software and services to a host of companies. It offers its wares on-premise and through the cloud. As most of us know, the deployment model in favor is the cloud, also known as a third party unless Samsung buys Nuance.

Warning from Samsung: This report appears to have been immediately followed by a warning from Samsung itself

- Nick Grimm, *Samsung warns customers new Smart TVs 'listen in' on users' personal conversations*, *ABC News*, 10 February 2015
- Eyder Peralta, *Samsung's Privacy Policy Warns Customers Their Smart TVs Are Listening*, *WEAA*, 9 February 2015;
- Nicholas Brown, *As The Internet of Things Grows, Samsung Warns Of Listening TVs*, 9 February 2015;
- James Dean, *Careful what you say, your TV is listening, warns Samsung*, *The Times*, 9 February 2015
- Andrew Griffin, *Samsung smart TVs listen to everything you say, warns privacy policy*, *The Telegraph*, 9 February 2015
- Brandon Russell, *Samsung updates its scary big brother always-listening TV policy*, *TechnoBuffalo*, 10 February 2015
- *Samsung smart TV issues personal privacy warning*, *BBC News Technology*, 10 February 2015
- *Not in front of the telly: Warning over 'listening' TV*, *BBC News Technology*, 9 February 2015).

These were apparently immediately followed by a modification to that policy statement (*Samsung tweaks policy after eavesdropping freak out*, *CNN*, 11, February 2015; Chris Matyszczy, *Samsung changes Smart TV privacy policy in wake of spying fears*, *CNET*, 10 February 2015). It had originally stated:

If your spoken words include personal or other sensitive information, that information will be captured and transmitted to a third party

As noted by Natasha Lomas ([Samsung Edits Orwellian Clause Out Of TV Privacy Policy](#), *TechCrunch*, 10 February 2015), it now includes a section explaining how voice recognition works. It says in part:

If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.) that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Samsung will collect your interactive voice commands only when you make a specific search request to the Smart TV by clicking the activation button either on the remote control or on your screen and speaking into the microphone on the remote control.

Commentaries: The issue was then the subject of commentaries, many of which appear to have been quickly "updated" (presumably following legal advice). A number made comparisons with the novel of [George Orwell](#) (*Nineteen Eighty-Four*, 1949), which depicted a nightmarish world of a state listening into its citizens. The following titles speak for themselves::

- Bruce Schneier, [Your TV may be watching you](#), *CNN News*, 12 February 2015
- David Goldman, [Your Samsung TV is eavesdropping on your private conversations](#), *CNN Money*, 9 February 2015
- Michael Cowling, [It's not just your TV listening in to your conversation](#), *The Conversation*, 10 February 2015
- Alanna Ketler, [Careful What You Say, Your Samsung Smart TV Might Be Listening](#), *Collective Evolution*, 18 February 2015; [Careful what you say: Your Samsung TV might be listening](#), *RT*, 11 February 2015
- Dominic Crossley, [Samsung's listening TV is proof that tech has outpaced our rights In light of Samsung's privacy notice](#), *The Guardian*, 13 February 2015
- Tyler Durden, [A Very Slippery Slope: Yes, Your Samsung Smart TV Can Listen To Your Private Conversations](#), *Zero Hedge*, 9 February 2015
- Dave Lewis, [Is Your TV Spying On You?](#) *Forbes*, 10 February 2015
- Parmy Olson, [Samsung's Smart TVs Share Living Room Conversations With Third Parties](#), *Forbes*, 9 February 2015
- Lauren Walker, [Shh! Your Smart TV Is Listening!](#) *Newsweek*, 9 February 2015

News reports -- apologetic and otherwise

Blaming the messenger: One response from Samsung has been to claim that its privacy policy had been "misinterpreted" by critics, rather than admitting that the criticism had been engendered by a fundamental lack of clarity in its own formulation -- whether deliberate or inadvertent. Who tests the comprehensibility of such policies and the "small print" of contracts governing purchase guarantees? As with the size of print, are they deliberately designed for minimal comprehensibility -- despite increasing recognition of hacking scandals associated with internet applications?

Whilst the naivety of potential buyers may be systematically exploited in the marketing process, to what extent could Samsung itself be considered naive -- as with other producers of such facilities? Or do vendors consider that there is sufficient lag time and minimal risk, allowing them to reduce costs by effectively outsourcing rigorous testing to hackers, enabling any detected vulnerabilities to be remedied at a later date?

Denial: One pattern of response to challenges by users naturally takes the form of denial:

- [Samsung rejects concern over 'Orwellian' privacy policy](#), *The Guardian*, 9 February 2015
- [Samsung Smart TVs Do Not Monitor Living Room Conversations](#), *Global Samsung Tomorrow*, 10 February 2015
- Chris Welch, [Samsung says its TVs aren't creeping on your living room conversations](#), *The Verge*, 10 February 2015

Minimizing the issue: With no possible indication of the factors which had influenced their perspective, a number of commentators have sought to minimise or relativise the issues highlighted by others:

- Michele Masterson, [Samsung Listens but Doesn't Sell Viewers Out](#), *Speech Technology*, 11 February 2015
- Larry Dignan, [Samsung SmartTV eavesdropping flap overblown](#), *ZDNet*, 9 February 2015 -- arguing that although a SmartTV may indeed share data from conversations with third parties, but this is hardly a matter of concern when the latter is a software provider converting speech to text
- Caleb Denison, [You can stop whispering: your Samsung Smart TV isn't spying on you](#), *Digital Trends*, 9 February 2015
- Samantha Murphy Kelly, [Samsung's TVs aren't the only devices listening to you](#), *Mashable*, 10 February 2015
- Guy Walters, [It's not just smart TVs. Your home is full of gadgets that spy on you: How internet giants are collecting your personal data through their high-tech devices](#), *Daily Mail*, 12 February 2015

"Everybody does it": Curiously -- echoing the argument with respect to phone hacking and large scale espionage, even amongst allies -- an argument is presented that in the emerging so-called "internet of things" everybody is implementing such invasive facilities (Charles Arthur, [Internet of Things: connect your TV, home, even your body, to the internet -- but beware hackers](#), *The Guardian*, 9 February 2015). In arguing that its privacy policy had been misinterpreted (as noted above), Samsung claimed that its voice recognition technology

(ssNLF) worked in a manner similar to Apple's (AAPL, Tech30) Siri, Google (GOOG) Now, Microsoft's (MSFT, Tech30) Cortana or any other speech-to-text service.

Indeed in a response by the writer by the vendor, it was claimed that smartphone technology (and the associated apps) was more invasive than that of the Smart TV.

Smart devices: As tends to be made clear in placing the issues of a Smart TV in the emerging technology context, the range of intelligent devices now includes (if only potentially):

- smart phones, which have been the subject of many reports
- personal computers, and the dubious role played by "cookies", supposedly to enhance web browsing
- smart cars, with the obvious potential of using GPS to enable targetted adverts -- as with the practice in sports arenas -- and to enrich the driver's profile, whether for subsequent marketing or analysis by security services
- smart toilets, with the possibility of monitoring medical conditions and their communication to to medical services and insurance agencies
- smart routers, with the legal complicity of ISPs in relation to marketing contracts and those with intelligence agencies
- smart fridges, cookers, and the like, with their potential monitoring of foodstuffs to facilitate marketing by suppliers
- intelligent houses, including all of the above, and more
- devices in supermarkets claimed to be in the interest of enhancing the shopping experience, but of remarkable value to enabling targetted advertising

Secret algorithms: In a special issue on *The Algorithms that Run Your Life*, commentary is included on the question *Secrets of the Home: Is Your Toaster Spying on You?* (*New Scientist*, 7 February 2015, p. 39) -- in addition to reference to the toothbrush, making the point:

With a smart system, the whole point is that when you use it, it learns about you over time... That learning intrinsically involves some sort of logging.... We may need to get used to the idea of no longer being at home alone.

With respect to the algorithms by which domestic devices are controlled, Hal Hodson (*No One in Control: the algorithms that run our lives*, *New Scientist*, 7 February 2015, pp. 31-33) makes the more general point:

Automated processes are no longer simply tools at our disposal: they often make the decisions themselves. Much of the news we read, the music we listen to and the products we buy are served up automatically, based on statistical guesswork about what we want. Invisible chaperones shape our online experiences. Systems we can't examine and don't understand determine the route we take to work, the rates we get for our mortgages, and the price we see for airfares. Many are proprietary and all are complex, pushing them beyond public scrutiny... Not only are most algorithms secret recipes, sometimes even the developers who wrote them are in the dark... Some think that hidden algorithms played a part in the 2008 sub-prime mortgage crash.... Automated systems are replacing human discretion in ever more important decisions... the documents leaked by Edward Snowden revealed that the National Security Agency uses algorithms to decide whether a person is a US citizen. According to US law, only non-citizens can have their communications monitored without a warrant... Depending on what you do online, your [assumed] citizenship might change overnight

As noted, many of the features offered may be especially designed for marketing services and security services -- whether or not these opportunities are clearly distinguished as engendering the secondary or primary income stream. Both the latter are variously dependent on ever more assiduous profiling. The most obvious consequence is targetted advertising by the former. In the latter case the user may become the target -- understood otherwise, if not fatally. As implied by the reference to the sub-prime mortgage crash, the obscurity of algorithms may well prove to be disastrous for civilization, as discussed separately (*Uncritical Strategic Dependence on Little-known Metrics: the Gaussian Copula, the Kaya Identity, and what else?* 2009).

Inspired by Bond movies, the permanently flashing light on this writer's electric toothbrush is a continuing reminder of ignorance as to how invasive technology may have become!

Disabling "smart features" and questionable "loss of settings"

Seeking deactivation: In the light of this controversy, one issue in the experience of this writer was determining how to disable the "smart features" in order to avoid the unknown implications of "voice recognition". Having been set up by the vendor's technician (and personalised by a helpful techy son), attention had been focused on the need to avoid turning the Smart TV off in order to avoid "loss of settings". Fumbling with two unfamiliar remotes (one for a set-top box), "turning off" frequently occurred. The issue was then how to determine whether voice recognition had indeed been activated or deactivated.

With respect to the superior model (not acquired) equipped with a camera, commentaries (including an early response from Samsung) responded to the issue of deactivation as follows:

Should the TV owner choose not to use these features, the camera and microphone can be disabled. Users can check if the camera and microphone are activated from the TV's settings menu. As an added precaution, the camera can be rotated and tucked into the bezel of the TV. Once tucked away, the camera only captures a black image. (Josh Kirschner, *Samsung Responds to TV Spying Concerns*, *Techlicious*, 2 April 2012)

Others noted that the lens of the camera could simply be "taped over". The challenge with respect to the voice-enabled version was what exactly could be done to deactivate it, effectively to "tape it over" -- or to ensure some form of "vasectomy" by "cutting its wires" (clearly a breach of contract however). When asked, the Samsung agent proved unable to demonstrate how deactivation could be achieved through the settings menu. Consideration was given by the writer to installing a "water feature" close to the TV microphone -- a form of interference long-publicised in Bond and other spy movies.

In the quest for safe intercourse over the internet, vasectomy offers one suggestive metaphor indicative of the need to ensure "safe sex", "cognitive contraception", and adequate protection against the consequences of invasive penetration by unwelcome parties. The parallel is also indicative of the future possibility that some agencies may adopt policies with a strong resemblance to those of the Catholic Church with respect to contraception. In the spirit of *Nineteen Eighty-Four*, it may be considered to be suspiciously unsociable and subject to sanction to deactivate voice recognition (or the video camera). The arguments of intelligence services are only too evident. Marketing of appliances, like TVs, could be priced on condition that they are permanently activated -- with no ability to deactivate them.

Concrete proof? In experimenting with the possibilities of deactivation of "voice recognition", the personal experience focused on determining whether the microphone was active or not. Most curiously this is not readily apparent -- in contrast with the icon commonly visible on a TV screen when the mute button is used to cut the sound from the speakers. A SmartHub button on the remote of the Smart TV brings up a coloured icon which immediately fades. It is completely unclear what aspects of this iconography signal that it has been turned on or off. Is it necessary to turn it on to determine whether it is off -- or vice versa? If a safety catch on a weapon were to depend on such feedback, it could of course be disastrous -- especially in the case of (dis)arming a missile launcher.

One alternative adopted was to shout at the screen (typically **"Help"**) since that had initially brought up a menu which appeared to be associated with control of voice recognition. However, despite shouting "Help" at the screen on subsequent evenings -- with no similar reaction -- there was no sense of confirmation that voice recognition had indeed been deactivated. Whether the neighbours may have thought there was a pattern of evening domestic abuse is another matter.

Recognition versus Recording? There is a further issue regarding "voice recognition", despite the claims of Samsung with regard to the role of third parties in interpreting information recorded, and the possibility of deactivation of that "recognition". The commentators seemingly say nothing about whether "voice recording" continues even when "voice recognition" is deactivated. Technically the distinction is between processing voice data for recognizable keywords, versus simply storing the recorded sound for possible later analysis -- whenever and by whatever means.

Such questions highlight the issue as to whether "deactivation" is defined in terms of "recognition" only -- but in no way excludes transfer of microphone input, although without any real-time processing. Thus according to the meaning of "voice recognition" (as conventionally known) deactivation may be limited to real-time processing. The "deactivation" procedure (if it can be readily found) may in no way imply that recording does not continue in some way. In contrast with the volume mute control, "off" may in no way mean "off". There is no concrete proof in this respect -- despite shouting **"Help"**.

Deactivation more generally: Such issues are clearly common to other devices. The writer had the experience of spending the night in a sophisticated Toyota rental car, in an airport parking lot, without being able to lock it from the inside -- without triggering the alarm. The smart software interpreted movement within the car, after locking, as the activity of an intruder for which an appropriately piercing warning sound was righteously generated. The car manual consulted in the middle of the night did not offer clear indication regarding the deactivation procedure.

It was necessary to leave the car door slightly ajar -- fortunately in a secure area in a mild climate. In the absence of concrete proof of success, experimenting with deactivation possibilities depended on the alarm being triggered (after a smart delay) -- clearly inappropriate in an airport parking lot with security patrols.

Forced deactivation? The EU is in a process of subjecting most energy using products on the markets of the EU countries with Ecodesign regulation. Products covered by regulations that are already in force are: standby and off-mode losses, simple set-top boxes, non directional household lamps, tertiary sector lighting products, external power supplies, electric motors, circulators, TVs, domestic refrigerators and freezers, household washing machines, household dishwashers, air conditioners and fans. With respect to "loss of settings", it may become a legal requirement that Smart TVs turn off automatically.

Dual purpose and Doublespeak: features vs exploitation

Dual-use technology: It appears clear that emerging forms of internet technology are best understood according to the classical term [dual-use](#). This refers to any technology which can satisfy more than one goal at any given time. With respect to smart devices, the duality of use is obscured by the promotional emphasis placed on the unusual features that they creatively offer to users. This typically disguises the extent to which these same technologies can be used to exploit those same users in ways that they do not suspect and which are far from being clearly articulated, if at all.

Embedding spyware: Even if suspicions are voiced, typically the implications will be denied to the extent possible. This has become progressively evident with regard to the extent to which spyware has been embedded in computer software and hardware for commercial and security purposes -- with the complicity of a variety of vested interests.

At the time of writing, as but the latest example, it is reported that Lenovo -- the world's largest PC manufacturer -- has been pre-installing [Superfish](#) in its products. This is a particularly pernicious form of adware that siphons data from a user's machine via web browser (Jose Pagliery, [Lenovo slipped 'Superfish' malware into laptops](#), *CNN Money*, 18 February 2015; Charles Arthur, [Lenovo demonstrates that malware is big business](#), *The Guardian*, 20 February 2015).

Misleading single-use hype: Within this industrial context, it is naive to imagine that Samsung has avoided strategies which operate in a

similar manner -- to the ultimate disadvantage of the user. The point which it appears necessary to emphasize is that new features are designed by the industry as a trap to tempt unsuspecting users -- a classical marketing ploy. The characteristic hype regarding such features should be recognized as a means of disguising the trap and the manner in which it is liable to exploit the gullible user. Put crudely and succinctly, new features should be recognized as an exciting way to screw and be screwed.

As has long been stated in the case of the internet, if it is free to the user it is most probable that the user is indeed intended as the product -- meaning the user's profile and the purchasing capacity it represents. New features can best be understood as having a two-way or bi-directional process embedded in them -- enabling what they claim to offer to some degree whilst exploring the user thereof to an unsuspected degree. Whilst the invasion of privacy for marketing purposes has been widely reported -- and widely accepted -- less evident is the manner in which such technologies are now deliberately developed and designed as a means of detecting security risks through extended profiling. This may be a constraint imposed upon the manufacturer (possibly according to security legislation) or a contractual arrangement with intelligence services from which the manufacturer may significantly benefit -- to the point of deliberately developing the technology in response to that income possibility.

Technological doublespeak: It is therefore appropriate for commentators on the Smart TV features to recognize parallels with the prescient account of *Nineteen Eight-Four* regarding the use to which the recorded information may be put by ill-defined third parties. In the language of George Orwell, the marketing of such technology is exemplified by an unknown degree of **doublespeak** -- in this case technological doublespeak.

Marketing of dual-use technology, under the banner of single use innovation, is clearly a means of disguising a secondary use -- one which may well have been conceived as primary from a research, development and marketing perspective.

Incomprehensible conditions? Especially interesting is the manner in which the marketing of sophisticated devices may disguise exploitation by inviting ready "agreement" with the conditions governing the legal guarantee. It is characteristic of the presentation of such conditions that they take the form of "small print" -- a term by which they are known. There is little expectation that these should be read by a purchaser although every reliance is placed on that wording in the event of problematic legal issues arising from its use. The conditions are typically crafted with the greatest legal skill to protect the vendor. The process can be readily recognized as progressively creating a condition in which the complexity of the small print, and the difficulty of comprehending it (even if legible) enable loop holes for the vendor to maximize exploitation of the purchaser -- most notably the elderly and the variously disabled.

As noted by the Samsung vendor to the writer, the small print could cover anything -- including unforeseen financial commitments -- since it was not designed to be read, and there was little expectation in marketing the product that it would indeed be read prior to a purchase.

Legal singularity versus Technological singularity: Seemingly unrelated, there is notable speculation regarding a future **technological singularity**, a hypothetical moment in time when artificial intelligence will have progressed to the point of a greater-than-human intelligence (Ray Kurzweil, *The Singularity Is Near: when humans transcend biology*, 2005). This predicts an exponential increase in technologies like computers, genetics, nanotechnology, robotics and artificial intelligence, leading to a point where progress is so rapid that it outstrips human ability to comprehend it. Kurzweil predicts that date to be 2045 -- a period which figures notably in various other reports of convergence of strategic concerns (resources, etc.).

With the emphasis on comprehension, and concerns regarding population aging, it might be asked whether such a technological singularity will be preceded by a form of "legal singularity". This would be one in which the conditions governing technological purchase, and the manuals describing their operation, effectively outstrip average human ability to comprehend them. The technological singularity could then be seen to be in process of being heralded by such a legal singularity -- effectively its harbinger.

Given his concern with the technological singularity, there is considerable irony to the fact that it was indeed Ray Kurzweil who achieved prominence in the initial development of voice recognition software -- within a corporation subsequently acquired by Nuance.

Legality of subsequent use of recorded information

Third party role: As noted in the commentaries above, Samsung has modified the wording of its privacy policy -- despite complaining that its original intentions had been misinterpreted. It has progressively become clearer that the verbal information captured via the Smart TV is passed to a third party, now more widely known to be **Nuance Communications** (*Nuance Brings Voice to Samsung Smart TV Line Up*, 9 May 2012). Headquartered in the USA, the corporation specializes in speech recognition and imaging applications. The company is claimed to be responsible for Samsung's "voice recognition". Less clear, as implied above, is whether Nuance also records information derived from a Smart TV, irrespective of whether it is obliged to process it in real time. Also less evident is what happens to the visual recordings in the case of the camera-enabled variant of the Smart TV.

The wording of the Samsung policy now reads:

You can control your SmartTV, and use many of its features, with voice commands. If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

Legal proof of deactivation? The point is made that users can of course disable these features by turning off voice recognition in the settings menu, but it appears that the third party contextual data collection cannot be disabled without losing the handy voice recognition service altogether. Again, whatever modification is made in the settings menu, there is no concrete proof that information is not being passed on to a third party anyway. This is a situation which has become familiar in the operation of personal computers and in ensuring constraints on such undeclared communications.

No concrete proof is supplied (or can be), making it extremely difficult to avoid suspicions of any form of dubious exploitation of information derived from users -- in this case from their living room use of a Smart TV, or from their bedrooms for that matter.

Undeclared involvement of other parties: Especially interesting is whether Nuance (or any other undeclared "third party") is then free to engage with other parties under commercial contracts -- or is obliged to do so under security legislation (as is typical of Homeland Security provisions in the USA). Clearly any verbal or other declarations in this regard are as credible as those which have been variously made by US-based computer and software manufacturers over the past few years -- only to be reframed when found to be less than credible in the light of emerging evidence. Denials of vulnerability to hackers have been feeble, without any provision for legal proceedings against vendors of such technology.

Would a fourth or fifth party on the information distribution chain hesitate in the face of the opportunity of using bedrooms scenes -- if an income stream could be ensured from such a source?

In his comment, Chris Matyszczy (*Samsung changes Smart TV privacy policy in wake of spying fears*, *CNET*, 10 February 2015) notes:

However professional Nuance Communications is (and it works with many companies such as LG and Panasonic to, for example, turn speech into text), there is always going to be a little doubt. There's certainly a question as to what happens once Samsung has passed your data to Nuance.

Nuance's privacy policy says, for example: "By using Nuance products and services, you acknowledge, consent and agree that Nuance may collect, process, and use the information that you provide to us and that such information shall only be used by Nuance or third parties acting under the direction of Nuance, pursuant to confidentiality agreements, to develop, tune, enhance, and improve Nuance services and products". Further in the privacy policy is a reference to data use for "advertising and marketing."

I have contacted Nuance to ask whether it feels able to pass voice data information -- in whatever form -- obtained via Samsung Smart TVs to third parties.

Future legal requirements: Irrespective of current concerns, also of relevance are the possible developments of the smart technologies and the requirements for their use. These may include the future legal requirement to have an "enabled" TV or smartphone -- with penalties for failure in this respect. A striking case in Germany has been the arrest of German sociologists, notably triggered by failure to bring their mobile phones to meetings -- interpreted, as with encryption of emails, as an indication that the meetings were of a suspicious nature from the perspective of the intelligence community (Richard Sennett and Saskia Sassen, *The War on Shapeless Terror*, *The Guardian*, 20 August 2007).

Clearly there are possibilities that some future personal insurance claims will not be honoured if the claimant fails to be able to prove use of a smartphone at the time. A similar situation may emerge with respect to medical claims under circumstances governed by social security legislation. Lobbies for the relevant technologies have a clear interest in promoting such legislation -- to whatever degree they may be complicit with the dubious requirements of the intelligence services.

Intellectual copyright: Also of interest is the possible evolution of intellectual copyright in relation to information collected by smart devices. Whose property -- in legal terms -- is the data passed by a Smart TV to Nuance? To what extent does conversation in front of a TV -- and disseminated to others -- constitute "publication", potentially subject to copyright? In other settings, as with respect to a conference speech, release forms are a common requirement before the content can be disseminated onwards. Does the Smart TV small print in fact constitute such a release?

Should concerned users be exploring the possibility of class action suits against such vendors for misuse of data beyond the provisions of the small print? Should users consider the need to face vendors with a legally binding non-disclosure agreement, prior to purchasing the technology -- especially for corporate boardrooms? On the other hand, use of a Smart TV to display movies and music (inappropriately downloaded and shared) could presumably be tracked via Nuance -- suggesting a major income stream in relation to those endeavouring to recover such lost income.

Copyright governing recorded imagery: The legal issues are all the more interesting with respect to recorded imagery. especially the cases in which a Smart TV is used in the presentation of business and strategic plans -- spreadsheets, diagrams, blueprints, and the like. Such devices are presumably widely used in boardrooms as a means of displaying reports and presentations from personal computers. How is such information processed by Nuance, especially given its expertise in [biometric facial recognition](#) for security purposes?

Could this be understood as an extension of processes of commercial espionage -- readily framed as in defence of the competitive advantage of the USA, and therefore of its national security? Will this result in the systematic identification and profiling of participants in strategic meetings -- as it may well do following installation of a Smart TV in the bedroom? Nuance may then seek to extend its databases of biometric data to include images of other portions of users' anatomy.

Security and intelligence implications: In relation to intelligence and security concerns, if the evolution of technology and legislation is to be understood as forming an integral part of the US need for [Total Information Awareness](#) (and [full spectrum dominance](#)), should the design and implementation of smart devices -- such as the Samsung TV -- be seen as part of a curious form of systematic enclosure of

private space? Another variant of the [tragedy of the commons](#)? As with personal computers more generally, should such devices and their associated applications simply be understood as "front ends" for a high-tech variant of the [military-industrial complex](#)?

Much has been reported on the keywords in email and blogs which are tracked by the intelligence services in seeking to determine "persons of interest". Given the warning of Samsung regarding personal conversations within the hearing of a Smart TV, is it evident what keywords might trigger response from clients to whom Nuance may transfer such information? Of particular interest is whether Nuance will be able to correlate use of derogatory keywords to viewing by users of declarations of a given politician -- articulating the policies of the USA for example. As part of extending program rankings for commercial purposes, in the light of channel choice by users, will such indications be used to enrich the sociopolitical risk profile of users -- for the benefit of the intelligence services?

There will of course be no concrete proof as to whether these possibilities are in place or envisaged. The past denials by CEOs regarding backdoor features are an indication of the pattern to be expected.

Smartening TVs and dumbing down content?

There is a curious irony to the exponential increase in the "smartness" of smart devices in comparison with what might be recognized as a rapid [dumbing down](#) of content -- and audiences. This is defined as the deliberate diminution of the intellectual level of education, literature, cinema, news, and culture. As movie-business slang, used by motion picture screenplay writers, it is understood to mean the revision of content to appeal to those of little education or intelligence. Whilst there is considerable focus on indicators of "smartness" of devices, there is little specific commentary on this trend, notably in relation to the exponential increase in program channels accessible via Smart TV.

Ironically the smartness of a Smart TV, as with other such devices, does not include being enabled for the elderly, for those with disabilities (technical or otherwise), or for those with multiple devices -- each requiring levels of attention which may distract from other challenging priorities. How much user training should a smart device require? How much training should manufacturers of such devices require in rendering user manuals comprehensible?

As notably cited by [Carl Sagan](#) (*The Demon-Haunted World: science as a candle in the dark*, 1996):

I have a foreboding of an America in my children's or grandchildren's time -- when the United States is a service and information economy; when nearly all the manufacturing industries have slipped away to other countries; when awesome technological powers are in the hands of a very few, and no one representing the public interest can even grasp the issues; when the people have lost the ability to set their own agendas or knowledgeably question those in authority; when, clutching our crystals and nervously consulting our horoscopes, our critical faculties in decline, unable to distinguish between what feels good and what's true, we slide, almost without noticing, back into superstition and darkness...

The dumbing down of America is most evident in the slow decay of substantive content in the enormously influential media, the 30 second sound bites (now down to 10 seconds or less), lowest common denominator programming, credulous presentations on pseudoscience and superstition, but especially a kind of celebration of ignorance.

A feature of dumbing down is clearly the incidence of advertising and the mass markets to which TV programs must necessarily be designed to appeal -- to maximize advertising revenues. In a global society acknowledged to be increasingly complex and faced with increasingly complex decisions, what is it that is minimized in dumbing down and what is it that is maximized to enhance audience attraction?

Dumbing down of wider concern: Such questions can be explored to some degree through the wider commentary on "dumbing down", as indicated below (and in the later [references](#)):

- Rich Blank, *Is Social Media Making Us Dumb? Social Media Today*, 31 July 2010
- John S. Driscoll, *Is our Free Press Being Dumbed Down? The Melrose Mirror*
- Frank Furedi, *Dumbing down? Don't blame the media, Spiked!* 15 December 2004
- Roy Greenslade, *TV news 'not dumbing down', says study, The Guardian*, 12 January 2012
- Joachim Hagopian *The Dumbing Down of America by Design, Global Research*, 14 August 2014
- Jonathan Holmes, *No need to dumb down on digital platforms, The Age*, 3 December 2014
- Susan Jacoby, *The Dumbing of America, The Washington Post*, 17 February 2008; *The Age of American Unreason: defining dumbness downward*, Center for Inquiry, 2012
- Tony Popowski, *Dumbing It Down for your Audience and Content Marketing, Grass Roots Marketing*, 21 August 2014
- Colleen Raezler, *'Dumb' Americans, Media Research Center*, 20 February 2008
- Tim Rich, *Is the Web Dumbing Us All Down? PCWorld*, 7 August 2010
- Daniel Taylor, *Electronic media and the dumbing down of society, Old-Thinker News*, 12 September 2007
- Daniel Taylor, *Ubiquitous Computing has Built Ultimate Surveillance Society, Old-Thinker News*, 23 March 2012
- Mick Temple, *Dumbing Down is Good for You, British Politics*, 1, 2006, 2, pp. 257-273
- Jay Tolson, *A Digital Dumbing Down? The lively debate over the intellectual impact of digital culture. U.S. News*, 28 August 2008
- Gillian D. M. Ursell, *Dumbing down or shaping up? New technologies, new media, new journalism, Journalism*, 2. 2001, 2, pp. 175-196
- Ray Williams, *Anti-Intellectualism and the "Dumbing Down" of America, Psychology Today*, 7 July 2014
- Shawn Paul Wood, *The Dumbing Down of National News, PRNewser*, 30 October 2013

- Oliver Wright, *Are we being dumbed down by 'news' from social media?* *The Independent*, 16 December 2014
- *The Television News Media in America: the dumbing down of a nation!* *Daily Kos*, 3 March 2012
- *Advertising in the Media: the threat of biased and 'dumbed down' content.* *Royal Economic Society*, April 2009
- *Why Mass Media Content is Dumbing Down*, *Digital Deliverance*, 15 September 2008

Paradoxical complementarity of smartening and dumbing down: There is an ironic complementarity between the relation to smartening devices and dumbing down users, indicated by contrasting trends:

- **deliberately increasing the smartness of devices**, like TVs, may effectively render users "dumber" through their increasing inability to comprehend how best to benefit from the necessary increase in complexity of such devices with their array of features. Users are effectively "herded" into dumber usage patterns, especially if their technical competence is challenged. This tendency also plays out with respect to the legality of provisions associated with the purchase agreement, of which relatively few will be aware or seek to be aware. Vendors of smart devices benefit significantly from any increase in the "dumbness" of the average purchaser -- a process obscured by astonishment at the relative sophistication of the young with respect to appreciation and manipulation of some features
- **deliberately dumbing down audiences and users** necessarily creates a social context in which the technology is appreciated as ever smarter -- due to the increasing failure to understand it, how to use it, or its wider implications. Ironically the process of dumbing down then creates the impression of technological innovation -- without a real need to ensure such innovation. The necessary innovation then shifts to that of marketing and presentation -- to promote the appreciation that real innovation is underway. The limited relevance of much technical innovation to the fundamental challenges of social change emphasizes this point -- especially with respect to the unquestioning Silicon Valley illusions regarding its own relevance to global poverty, governance, and the like.

The interplay of smartening technology and dumbing down people could be seen as implied by the valuable study by [Noam Chomsky](#) and [Edward Herman](#) (*Manufacturing Consent: the political economy of the mass media*, 1988) -- notably through extension of "manufacturing" to include smart devices. Illusions regarding global governance, and the threats necessary to uncritical appreciation of authority and expertise, are fruitfully cultivated by shifting the balance between artificial intelligence and human intelligence (*Ungovernability of Sustainable Global Democracy?* 2011; *Promoting a Singular Global Threat -- Terrorism: strategy of choice for world governance*, 2002).

Anticipating a future device-enabled revolution in dialogue: Whether enabled for sound and/or vision, especially intriguing are the envisaged possibilities for dialogue with artificial (virtual) agents through such devices and their enabling software. Prototypes under development have already been demonstrated. Kubrik's *HAL 9000* offered an early sense of pros and cons -- as have other forms of science fiction. Educational variants are enthusiastically discussed. The crafting of online filter bubbles by algorithms is already evidence of the viability of "personalization" (Eli Pariser, *The Filter Bubble: what the internet is hiding from you*, 2011).

A number of authors have addressed the sense of isolation which internet possibilities obscure ([Sherry Turkle](#), *Alone Together: why we expect more from technology and less from each other*, 2012; [Ethan Zuckerman](#), *Rewire: digital cosmopolitans in the Age of Connection*, 2013). Loneliness, solitude and boredom are major issues for the elderly -- if not for the young. It is therefore intriguing to consider how quickly applications will emerge to enable dialogue with a virtual friend and how sophisticated these may come to be (*Forthcoming Major Revolution in Global Dialogue: challenging new world order of interactive communication*, 2013).

Less evident is the probable trend towards crafting intelligent agents with a particular bias -- whether education, religious, commercial or political. The interest in such possibilities has been made evident in the documented cultivation of Hollywood by the Pentagon. The process could be further extended to address issues of indoctrination and (de)programming -- in support of "values" variously defined in relation to security interests. Might the living room then offer processes analogous to those of confessional, vocational guidance, psychotherapy, or interaction with a political commissar -- or an agent of the security services?

Surveillance "mirrored" -- by whom, for whom? A [culture of fear](#) and confusion favours reliance on the intelligence of a smart environment -- increasingly acclaimed as being of a higher order than the society which sustains it, and extending to fantasies regarding a [global brain](#). Arguments have been fruitfully presented by [Evgeny Morozov](#) (*The Net Delusion: the dark side of internet freedom*, 2011; *To Save Everything, Click Here: the folly of technological solutionism*, 2013). Ironically, however, the natural environment, as framed by extensions of the [Gaia hypothesis](#) to the noosphere, may well prove to be characterized by an even higher order of intelligence -- understood in systemic terms.

Given widespread debate about global surveillance and monitoring -- especially its invasive nature, however justified -- there is huge irony to the curious complementarity between the following interpretations:

- with respect to the natural environment and the variety of emerging challenges and risks (climate change, endangered species, resources, etc)
- with respect to the psychosocial environment and its risks (*World of Work Report*, *World Health Report*, *World Education Report*, etc)
- with respect to security and associated risks (*Global State of Information Security*, etc)
- with respect to the capacity of the living-room user of the internet to monitor and survey the condition of the world using smart devices and applications (*Google Trends*, etc)
- with respect to the capacity of smart devices to monitor the living-room user for marketing and security purposes

In creating the user's illusion of the capacity to monitor the globe from the living room -- effectively putting the world to question -- the living room is transformed into an interrogation room. This is virtually indistinguishable from a police interrogation room (with a one-way

window) in which the user is effectively "put to the question" by unknown interrogators -- possibly algorithmically driven.

References

Mark Bauerlein. *The Dumbest Generation: how the Digital Age stupefies young Americans and jeopardizes our future*. Tarcher, 2008

Nicholas Carr:

- *The Shallows: what the iInternet is doing to our brains*. W. W. Norton, 2011
- *The Glass Cage: automation and us*. W. W. Norton, 2014

Noam Chomsky and Edward Herman. *Manufacturing Consent: the political economy of the mass media*. Pantheon, 1988

John Taylor Gatto. *Dumbing Us Down: the hidden curriculum of compulsory schooling*. New Society Publishers, 2002

Richard Hofstadter. *Anti-Intellectualism In American Life*. Alfred Knopf, 1964

Charlotte Thomson Iserbyt. *The Deliberate Dumbing Down of America*. Conscience Press, 2011

Maggie Jackson. *Distracted: the erosion of attention and the coming Dark Age*. Prometheus Books, 2009

Evgeny Morozov:

- *The Net Delusion: the dark side of internet freedom*. PublicAffairs, 2011
- *To Save Everything, Click Here: the folly of technological solutionism*. PublicAffairs, 2013

Ivo Mosley (Ed.). *Dumbing Down: culture, politics and the mass media*. Imprint Academic, 2000

Resulhan Öztimur. *Dumbing Down as Content Portfolio Strategy: a comparison of public and private TV broadcasting in Germany*. Diplom.de, 2009

Eli Pariser. *The Filter Bubble: what the internet is hiding from you*. Penguin, 2011 [[summary](#)]

Neil Postman:

- *Amusing Ourselves to Death: public discourse in the Age of Show Business*. Penguin, 2005
- *Technopoly: the surrender of culture to technolog*. Vintage, 1993

Charles Sykes. *Dumbing Down Our Kids: why American children feel good about themselves but can't read, write, or add*. St. Martin's Griffin, 1996

Sherry Turkle. *Alone Together: why we expect more from technology and less from each other*. Basic Books, 2012

Jean M. Twenge. *The Narcissism Epidemic: living in the Age of Entitlement*. Atria Books, 2010

Katherine Washburn. *Dumbing Down: essays on the strip-mining of American culture*. W. W. Norton, 1996

Ethan Zuckerman. *Digital Cosmopolitans: why we think the internet connects us, why it doesn't, and how to rewire it*. W. W. Norton, 2014



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](#).

For further updates on this site, [subscribe here](#)