Through the looking GLΛSS: Google Glass™, privacy, and opacity, with an Israeli law twist

Arye Schreiber*

Being transparent about GLΛSS

In 1787 the Founding Fathers or today, Parents, of America assembled in Philadelphia to adopt the Constitution. At the same time, Jeremy Bentham and his brother Samuel came together in what is now Belarus and thought up the Panopticon. Managing the clash between liberty and surveillance is, in a nutshell, what privacy law is about. Equilibria are found at which liberty and surveillance can co-exist, but these are disrupted from time to time, especially by social change and technological change. Examples of social change affecting privacy law would include war, changes in government, women's rights, free press, economic forces, and more. Examples of technological change include trains, linotype presses, telegrams and telephony, computers and the internet. Much has been written about the pervasiveness of recent technological developments that challenge and endanger our privacy, from social networking to biometric databases.[1] Privacy vis-à-vis government has come sharply into focus following recent revelations of PRISM and Tempora, details regarding the domestic use of drones in the USA, and the use of CCTV in the successful hunt for the Boston bombers.

This article focuses on one emerging technology that has the potential to alter considerably the privacy landscape—namely, Google GLΛSS. Glass is essentially a tiny computer on a frame of spectacles. Also attached are a miniature display, which sits atop where a spectacles' lens would normally be; a camera; a microphone; and a bone-conduction transducer, which is a kind of subtle little speaker beside the ear; and a GPS. It also contains a light sensor, a proximity sensor, Bluetooth connectivity, an accelerometer, a gyroscope, and a magnetometer. Glass runs the Android operating system, and apps—called Glassware—are being developed for Glass much as they are for smartphones. Glass is not yet commercially available as of the time of writing, but has been

Abstract

- Google Glass™ and other wearable computers pose considerable challenges to existing privacy paradigms and laws. This article examines Glass and its implications for privacy from an Israeli law perspective. The article focuses on privacy of third parties vis-à-vis the Glass user, rather than on the privacy of the user vis-à-vis others or the state.
- Privacy law concerning visual privacy—taking and publishing pictures of others—needs to meet the wearable computing challenge. As wearable computers become ubiquitous, 'reasonable expectations of privacy' will change. The law will likewise need to accommodate a new reality in which an inconsequential passing glance becomes a recording saved for posterity, and possibly shared with the world in real-time. The author suggests that there are good grounds for recognizing a Right to Opacity—a right not to be subjected to constant surveillance and photography.
- Eavesdropping law will need to evolve in order to contend with new paradigms of intercepting conversation, including lip-reading and speech-to-text technology. These and other technologies that Glass will feature do not currently fall neatly within eavesdropping and privacy law definitions.
- Regulators and lawmakers around the world have responded inconsistently to Glass, apparently reflecting some fear, confusion, and suspicion. To the extent that regulators and legislators want some sort of consultative or veto rights over new products with privacy implications, that needs to be debated and legislated.

* Arye Schreiber, Schreiber & Co. Privacy and Cyberlaw <www.schreiberlaw.co>. Dedicated to the memory of Dr Abraham M Fuss, outstanding lawyer, scholar and uncle.

1 For a fine summary, see Omer Tene, 'Privacy: The new generations' (2011) 1 *International Data Privacy Law* 15.

distributed to many developers and technology thought-leaders amid a very successful media blitz, as a result of which many thorough reviews are available. There are competing technologies,[2] but Glass is likely to be the most impactful of its genre so it will be the central focus of this article, though much of the following analysis applies similarly to other emerging technologies.

Glass marks the beginning of a major new trend in technology that is differentiated from the smartphone paradigm in several important ways.

Several trends converge in Glass to give it unique potential for facilitating invasions of privacy. First, Glass is a wearable device. It is designed to be used and operated more or less all the time. One simply wears it while going about one's day. Other wearable devices, notably smart watches, will likewise begin to change the way computing, phones, and cameras are more integrated into our everyday lives. Studies show that most (72 per cent) smartphone users, at least in the USA, remain within a few feet of their phones at almost all times,[3] and in that sense Glass is nothing new. However, even when a smartphone is in a user's pocket, it is not readily usable, it needs to be removed from the pocket, unlocked, and activated before it is ready to, say, take a picture. Glass by contrast is designed to be in more or less perpetual readiness while it is worn, like spectacles. It is integrated into everyday living. A phone is plainly an external gadget, but many—the present author included—actually wear spectacles all our waking hours. One carries a phone, but one wears glasses. Wearable, omnipresent devices represent a considerable step-up in the ubiquity of technology in our lives and in the presence of potential privacy harm. Second, Google is one of the companies with the most potential to harm privacy, given its comprehensive access to and control of the data in the lives of so many people and institutions. Gmail users frequently integrate email, contacts, photos, calendars, documents, social network activity, search activity, location activity, and much more all working through Google services. The convergence of these two elements—the new form of the hardware, together with the services with which it is integrated—makes Glass uniquely capable of facilitating invasions of privacy.

This article will consider the impact of Glass on privacy—specifically privacy between citizens—through the prism of Israeli privacy law. The following analysis is divided into three parts. The first is a legal analysis of Glass under Israeli privacy law, with particular emphasis on visual invasions of privacy. There follows a brief analysis of Glass with respect to invasions of privacy through eavesdropping. Finally, the article relates how Data Protection Authorities and the US Congressional Bipartisan Caucus have reacted to Glass, and considers the sagacity and implications of those reactions.

Visual privacy

Glass is first and foremost a visual device, and raises considerable concerns with respect to its potential for visual invasions of privacy, and possible failures of existing law to catch those invasions. Section 2 of the Israeli Privacy Law 1981 (the 'Privacy Law') provides a closed list of invasions of privacy, civilly and criminally actionable. Two of these—sections 2(3) and 2(4)—are examined in this section with reference to Glass. A unique feature of Glass is that it integrates with what you already see—for example superimposing navigation directions on top of the topography you see. It also has a camera, and can therefore not only provide information that meshes with your vision, but can also extract information from your environment, for example—what and whom you see, and where, and these features of Glass will be pertinent to the discussion that follows.

Section 2(4) of the Privacy Law prohibits 'Publishing a person's photograph under circumstances, in which the publication is likely to humiliate him or to bring him into contempt'. This section has been the subject of much poignant litigation. One case that is particularly telling for this analysis is *Anon v Amnon Levi*.[4] Israeli family law is determined, for Jews, by Jewish religious law. Under ancient Jewish law—made famous by Biblical episodes such as Judah and Tamar, or Ruth and Boaz—a childless widow should marry the brother of her deceased husband—a levirate marriage, and this in ancient times was a safety net for the widow as well as a way to preserve the legacy of the deceased husband. Under the rules of levirate marriage, a brother who elects not to marry the widow was shamed in court in a ceremony called *halitza*. Today, levirate marriages are not conducted, but the ceremony is, though it is a technicality and today carries no shame with it. In *Anon* a widow appeared before the religious court to conduct the ceremony, and discovered to her horror that there were one hundred or so observers in the room. The ceremony went ahead and was very embarrassing for the widow, who was distraught, crying and barely able to

2 Notably: Vuzix, Sony, Epiphany Eyewear, GlassUp, Oculon Optoelectronics, Olympus, as well as many augmented reality innovators.

3 John Koetsier, 'Americans love their smartphones more than sex, showering or church' (*Venturebeat*, 11 July 2013) <http://venturebeat.com/2013/07/11/americans-3-their-smartphones-more-than-sex-showering-and-church/> accessed December 15, 2013.

4 Various Civil Petitions (Supreme Court) 6803/09 *Anonymous v Amnon Levi, Itai Dankner, Israel New Channel 10 Broadcasting Ltd.* (unpublished).

function. Onlookers were so uncouth as to film the event, and the footage made its way to the respondent television producers. She sought a temporary injunction barring airing of the footage in a documentary, pending a decision in a lower court. At the Supreme Court, Rubenstein J's hands were largely tied, since the pictures with the widow's face visible were already on the internet. Likewise, the producers had a section 18(3) defence of public interest. He ordered that particularly degrading parts of the footage be omitted. The pertinent point from this case is that unlawful, surreptitious photography dramatically changes the scope of privacy protection. Within seconds of such an event footage can already be in the public domain, and could already be in the hands of the press. Though this was not raised in *Anon*, the language of section 2(4) supports this conclusion: 'the publication is likely to humiliate him . . .', that is, if where the picture has already been published, additional publication may not meaningfully humiliate the victim further. The immediate publication of a humiliating picture or film thus largely undermines any effort at protection of privacy. As photography becomes routine, ubiquitous, and constant—which Glass advances considerably—there will be countless embarrassing moments like these that enter the public domain and simultaneously come within freedom of speech protection in near real time. In those circumstances protection of privacy is largely moot. In short, Glass undermines privacy by placing privacy-violating material in the public domain and bringing it within freedom-of-speech defences in near real time, largely bypassing the law that protects privacy.

Section 2(3) prohibits 'Photographing a person while he is in a private domain'. Under this section the photograph must be of a 'person', so photographing a person's intimate items for example, would not constitute a violation of section 2(3).[5] Likewise, there is a qualifier of 'private domain'. Israeli courts have ruled[6] that a person who is in the public domain could still be considered in the 'private domain' for the purposes of the Privacy Law if, at that time, they have lost control of their circumstances. The court gave some examples: if a person is involved in a car crash on a public road, or in a terrorist attack, or on account of some trauma lies helpless in the street in an exposed manner, that would be considered in a 'private domain' even though they are in a public place. Likewise, if a woman walks in the street, trips and falls on her face, and in the process her underwear is exposed, she will also enjoy the protection of section 2(3) should someone happen to photograph or film her. By contrast, a woman sunbathing on a public beach may be photographed.[7] The Supreme Court, in the appeal of the same case, ruled that a photograph of a person that also shows some of his personal details—in that case a person was photographed at work selling books in his store—would be caught by section 2(3).[8]

Israeli Supreme Court case law indicates that the test for 'private domain' is akin to the 'reasonable expectation of privacy' test familiar from US law,[9] such that a secluded area in the woods could be a 'private domain' for these purposes.[10] Note that section 2(3) does not require publication of the photographs. Taking photographs is sufficient to constitute a tort, actionable without need for proving any damage.[11]

The Privacy Law makes most violations of privacy, when coupled with intent, a crime (sect. 5). Therefore, assuming there is intent, sections 2(3) and 2(4) describe not only actionable torts, but crimes and therefore prohibitions. Note that an additional limitation of section 2(3) is that it does not prohibit installation of surveillance equipment, as noted by Halm.[12] In Halm's opinion, based on case law, this section ought to have been drafted to reflect, *mutatis mutandis*, section 2(c) of the Eavesdropping Law 1979 (the '"Eavesdropping Law'); that section prohibits installing eavesdropping equipment. However, the prohibition on installing eavesdropping equipment is without parallel in the Privacy Law, meaning that under the current law surveillance equipment could be installed, and only actual filming would be unlawful. Respectfully, Halm's suggestion is too far reaching. Workplace video, or visual surveillance is growing in Israel,[13] and courts have repeatedly stated that the installation of cameras is not a violation per se despite the fact that Israeli courts have

5 Section 2(11) would cover personal items, and in a recent case the Supreme Court found that publishing a computer simulation of the inside of a person's home constituted an invasion of privacy; Civil Appeal 1697/11 *Gotesman v Vardi* per Fogelman J, para. 15.

6 Civil File 199509/02 *Menashe Dror Zadik v Haaretz Newspaper Publishing Ltd*. The case went on to the District Court (Civil File (District, Tel-Aviv) 1978/04 *Menashe Dror Zadik v Haaretz Newspaper Publishing Ltd.*) and that ruling was partially overruled, but not on this point, by the Supreme Court in Civil Appeal 6902/06 *Menashe Dror Zadik v Haaretz Newspaper Publishing Ltd*.

7 These rather chauvinistic examples were given, curiously, by Judge Judith Shevach.

8 Supreme Court ruling in *Zadik* (n 6).

9 *Katz v United States* 389 U.S. 347, 362 (1967) (Harlan J).

10 Criminal Appeal 28436/05 *Sabri Jerais v State of Israel* [11] (Arbel J).

11 Privacy Law, section 29A.

12 Eli Halm, *Privacy Law* (Perlstein-Ginnosar 2003) 92.

13 See sources and discussion in Michael Birnhack, 'Surveillance at Work: Taylor, Bentham and the Right to Privacy' (2010) 12 *Labor, Society and Law.* In particular, see discussion at n 36 of the growing trend of surveillance at work.

given 'private domain' a very broad interpretation,[14] such that a person's office space at work could be their 'private domain' for the purposes of section 2(3) of the Privacy Law, even vis-à-vis the actual owner. In other words, the law prohibits filming, and the courts have extended that by broadening the meaning of the 'private domain'. But the courts generally recognize that installing equipment may be necessary to protect a person or institution's legitimate interests.[15] As demonstrated by several cases, surveillance equipment often needs to be installed, but its activation is governed by section 2(3). Dr Ludmila Leshziner was working as a physician in an old-age home, when the administration installed a surveillance camera overlooking her office space ostensibly to prevent recurring thefts. The doctor resigned, claiming severance because of a material deterioration in her employment conditions on account of the cameras. The cameras were operational throughout the day. The court noted that even if the doctor did not receive patients at that desk, and even if that desk was used by others in her absence, since she was not a suspect in the theft (which may have given rise to a defence for the employer), that space was her 'private domain'.[16] The doctor claimed that installing and operating the cameras was a violation of her privacy.[17] But the ruling, in her favour, notes that 'there was no justification for *activating* the cameras while the [doctor] was present and/or working in the room'.[18] The court thus emphasized that it was the operation of the cameras that violated her privacy.

In *Malul*, the same court, with a different bench, limited *Leshziner* to employees' personal work space, such that the opposite conclusion would be reached concerning shared and open office space.[19] *Malul* further cited *Leshziner* as relating to activating cameras, not to installing them, reemphasizing that installing cameras is not in itself an invasion of privacy. In both cases the court noted that use of surveillance equipment was justified—on account of thefts in *Leshziner* and on account of dangerous persons entering the office in *Malul*, but in *Leshziner* the cameras were directed at an individual's work space, and using the cameras while she was working was not justified since she was not a suspect in the thefts.

Halm is right, however, to note that the very installation of surveillance equipment is problematic. To understand why, and to see how that is relevant to Glass, a quick detour to some of the foundational contributions to privacy law is in order. Warren and Brandeis[20] wrote of the need for privacy law to be designed 'to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity'. Throughout their article their concern was with publication, not with solitude. Although they discussed the 'inviolate personality', they envisaged being 'let alone' as, basically, not having one's personal affairs published.

Prosser's famous division of four separate heads of privacy brought privacy closer to the emotional plane. His 'Intrusion upon Seclusion' tort expressly requires an invasion, but not a publication:

> The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.[21]

Missing from Warren and Brandeis, and likewise from Prosser, is consideration for the subjective feeling of being the object of surveillance. Though it is not currently the law in Israel, consideration must be given to making it an actionable invasion of privacy when another gives one the feeling that she is being observed and recorded, even if that is not necessarily true. As Michel Foucault argued,[22] the power of the Panopticon is in that it induces in the inmates a consciousness of being watched, in Yar's words, the 'visibility of visibility'. It is the uncertain feeling, the suspicion that at any time someone is watching, that disciplines conduct in the Panopticon. As Birnhack poignantly stated, 'many workplaces in the capitalist society of the twenty-first century are arenas of constant, precise and long-term surveillance of employees by their employers'.[23] And recent research points to just how effective that can be.[24] Though

14 See *Jerais* (n 10).

15 As an alternative, Halm's suggestion could be adopted, but courts would apply a section 18(2)(c) legitimate-interest defence very broadly.

16 Local Labor Court (Haifa) DMR 39840–04–10 *Ludmila Leshziner v Peer Center for Medical Recovery Ltd.* (2011).

17 Ibid. para. 26.

18 Ibid. para. 28, emphasis in the original.

19 Local Labor Court (Haifa) SA 15540–09–09 *Zehavit Malul v Roni Amar Account Management Services Ltd.* (2013).

20 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

21 Second Restatement of Torts sect. 652B; see also William L Prosser, 'Privacy' (1960) 48 California Law Review 383, 389–92.

22 See discussion in Majid Yar, 'Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis' (2003) 1/3 Surveillance and Society 254–271, 261.

23 Michael Birnhack, 'A Quest for A Theory of Privacy: Context and Control' (2011) 51/4 *Jurimetrics* 447–79, 411. Cited also in Regional Labor Court (Tel Aviv) Labor File 2723/09 *Shemuel Jubani v Si Siyurim (1986) Ltd*, at para. 7.

24 Lamar Pierce, Daniel C. Snow, and Andrew McAfee 'Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity' (30 August 2013), MIT Sloan Research Paper.

surveillance can be very effective for ensuring conformity through engendering a feeling of being watched, it is that exact same feeling that is so troubling to ordinary citizens, whether the purported watcher is the government or another citizen. CCTV is commonplace, and its role in the search for the Boston bombers has highlighted just how much citizens are being watched.[25] Yet for all the CCTV recordings of our everyday lives, all those images generally go unnoticed, unused, irrelevant, into an obscure hard drive somewhere. By contrast, Glass is designed to constantly interact with its environment. Glass not only observes and even records, as CCTV does, it also acts and reacts.

Israeli law in its current form is not well aligned to protect privacy from something like Glass, since the law does nothing to prevent such a 'feeling of being observed'. This gap is evident from the Database Registrar's guidelines on management of CCTV systems (the 'Guidelines').[26] According to Guideline 2.6, CCTV systems capable of licence plate recognition or facial recognition even with just 20 per cent success, and other forms of cross-reference with other databases, or systems with high resolution that would enable someone to recognize subjects from other photographs, all come within the Privacy Law and are caught by section 7 thereof, meaning they form databases including personal information and must be registered, and meet the many requirements of the law of such databases. Birnhack makes the point that the EU's Directive 46/95 is based on a database paradigm of information storage. He continues:

> [T]he Directive's database-based shortcoming is that there are emerging technologies which do not use a database at all, but nevertheless process our personal data. These systems act upon the data immediately, rather than store it in a database, such as biometric identification methods.[27]

Glass is a near-perfect example of such a technology. Glass can work out what we are looking at and how we feel about it without any need for a database (it can also take endless pictures and put them in a database of purely personal use which, pursuant to section 7, would bring the database outside of the scope of the Privacy Law).[28] Apparently the Registrar is aware of this loophole, and the Registrar published some Questions and Answers regarding the Guidelines, including the following (my translation):

> A camera which is not recording is not creating a 'database' and therefore the guidelines do not apply to it directly and fully. . . . Notwithstanding, operating a camera that does not record in the public domain creates a concern (*hashash*) for an invasion of the privacy secured and protected in section 7(a) of the Basic Law: Human Dignity and Liberty and in chapter 1 of the Protection of Privacy Law. Therefore, the principles and guiding themes detailed in the Guideline[s] can serve as a valuable tool also for one who operates such a camera [ie that does not record, A.S.] and seeks to respect the privacy of the people filmed and to act in accordance with the provisions of the law.[29]

It seems that this passage is telling; the Registrar believes that placing someone under CCTV surveillance ought to be regulated whether or not a database is created. The registrar did not explain how, where there is no database, there is a 'concern' for a possible invasion of privacy under the quasi-constitutional Basic Law or the Privacy Law. It appears to be the point noted above; that even where someone is not actually being observed or photographed, by creating a feeling that they are, one violates their privacy, if not under the Privacy Law, then under the Basic Law: Human Dignity and Liberty which increases considerably the scope of privacy protection in Israeli law beyond the provisions of the Privacy Law.[30]

Recognition of such a tort and/or crime and a corresponding 'Right to Opacity', or whatever we may call it, would be new. But new technologies such as Glass may require such a step. Calo has cogently suggested[31] that drones may just spark a move to new paradigms of privacy:

> Daniel Solove has argued that the proper metaphor for contemporary privacy violations is not the Big Brother of Orwell's 1984, but the inscrutable courts of Franz Kafka's The Trial. I agree, and believe that the lack of a coherent mental model of privacy harm helps account for the lag between the advancement of technology and privacy law. There is no story, no vivid and specific instance of a paradigmatic privacy violation in a digital universe, upon which

25 Terry Atlas and Greg Stohr, 'Surveillance Cameras Sought by Cities After Boston Bombs' (*Bloomberg News*, 29 April 2013) <http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html> accessed December 15, 2013.

26 Registrar Guidelines 4/2012: <http://index.justice.gov.il/Units/ilita/subjects/HaganatHapratiyut/MeidaMerasham/Hanchayot/42013.pdf> accessed December 15, 2013.

27 Michael Birnhack, 'Reverse Engineering Informational Privacy Law' (2012) 15 Yale Journal of Law and Technology 24, 89.

28 Conversely, the meaning of 'personal use' may be shifting, as government agencies apparently have access to many of our personal online storage facilities, as does the database processor (say, Dropbox, Google, Amazon).

29 <http://index.justice.gov.il/Units/ilita/faq/Pages/Camera.aspx> accessed December 15, 2013.

30 Omer Tene, 'The Right of Privacy under the Basic Law: A Conceptual, Legal and Regulatory Turning Point' (2009) 8 Kiryat haMishpat Ono Academic College Law Journal 39–70.

31 M Ryan Calo. 'The Drone as Privacy Catalyst' (2011) 64 Stanford Law Review Online 29.

citizens and lawmakers can premise their concern.

Drones and other robots have the potential to restore that mental model. They represent the cold, technological embodiment of observation. Unlike, say, NSA network surveillance or commercial data brokerage, government or industry surveillance of the populace with drones would be visible and highly salient. People would feel observed, regardless of how or whether the information was actually used. The resulting backlash could force us to reexamine not merely the use of drones to observe, but the doctrines that today permit this use.[32]

Calo's main point is that people 'would feel observed, regardless of how or whether the information was actually used' and that is true *a fortiori* for Glass, quite literally an 'in your face' surveillance technology, more 'visible and highly salient' even than drones. Satellites are remote, drones less so, CCTV is closer still, but Glass is about as close as can be.

As noted above, Glass and similar new technologies can add dramatically to the feeling of being watched. They also turn insignificant *de minimis* invasions of privacy into lasting, irreparable harms. These two impacts on privacy are considerably amplified by an additional emerging technology—facial recognition. Google has said it will not approve facial-recognition Glassware, but hackers have already got facial recognition software to run on Glass, and in a June 2013 letter (discussed below) Google wrote '. . . we won't be approving any facial recognition Glassware' adding the qualifier 'at this time'.[33] Google is obviously aware of the potential harms of facial-recognition technology on a consumer product.[34] Eric Schmidt, Google's chairman, recently said that Google 'built a facial-recognition tool. It was just really good—state of the art at the time. We stopped that product for two reasons. One is that it turned out to be illegal in Europe and the second was that it was not a good product to offer in the US for the same reasons. . . . Facial recognition, completely unmonitored, can be used for very bad things. It can be used for stalking, for example. You know, it's just we don't want to be part of that as a company. There are cases where facial recognition can be used, but they need to be fairly carefully boxed.'[35] Once workarounds are found to enable Glass to run facial-recognition apps, presumably Google will sooner or later succumb, support and even innovate in that space.

We see then that Glass largely avoids tortious and criminal provisions established in chapter 1 of the Privacy Law, specifically sections 2(3) and 2(4), and likewise is not generally caught by the chapter 2 database provisions. An additional avenue for privacy protection in Israeli law is constitutional law, specifically section 7 of the Basic Law: Human Dignity and Liberty. As emphasized by Barak CJ in a landmark Supreme Court case, beyond the provisions of the Privacy Law, case law and the quasi-constitutional protection of the Basic Law will extend the scope privacy protection.[36] The scope of constitutional privacy protection cannot be predicted, but the courts may use the Basic Law to interpret the Privacy Law much more broadly than would otherwise be plausible, and may use that as a tool for contending with new technologies that the Privacy Law alone, in its current form, cannot properly regulate.

In summary, everyday use of Glass may largely sidestep the Privacy Law provisions. The Privacy Law outlaws or makes actionable taking pictures of another in the private domain, but does not do the same for installing and using the equipment for such pictures. As to the database aspects of the Privacy Law, use of Glass per se will also not generally be governed by the database provisions of the Privacy Law. However, Israeli law, perhaps through constitutional provisions, could recognize that inducing in another the feeling of being observed could in itself—without any actual observation—constitute an invasion of privacy. This is one of the emerging areas of privacy law that may change with the spread of Glass.

Refraction—how Glass can change visual privacy law

There are several additional specific ways in which Glass challenges and changes the Israeli privacy law.

Again, section 2(3) prohibits 'Photographing a person while he is in a private domain'. Courts interpret 'private domain' very broadly, and in a context-specific way. A recent Magistrates court decision concerned one Guy Sanin who had been surreptitiously video-filming couples making-out in their cars in a public car park in Tel Aviv.[37]

32 Ibid., footnotes omitted.

33 Emphasis added.

34 So is the market, see Daniel Bates, 'How to stop Google Seeing you: Scientists produce "Anti-Glass" specs that Block eye-war technology' (*Daily Mail*, 26 June 2013) <http://www.dailymail.co.uk/sciencetech/article-2348178/How-stop-Google-seeing-Researchers-produce-Anti-Glass-specs-BLOCK-eye-wear-technology.html> accessed December 15, 2013.

35 James Ball, 'Google CEO Schmidt calls for end to private drone use' (*The Raw Story*, 20 April 2013). <http://www.rawstory.com/rs/2013/04/20/google-ceo-schmidt-calls-for-end-to-private-drone-use/> accessed December 15, 2013.

36 SCJ 6650/04 *Anonymous v Netanya Regional Rabbinic Court et al* Tak-Al 2(2006) 1736, para. 8 et seq. See at length Tene (n 30) p. 48 et seq.

37 Criminal File (Tel Aviv, Magistrates) 22744–09–11 *Guy Sanin v State of Israel*, delivered 4June 2012.

He was charged with an offence under section 2(3), and claimed that the victims were not in a 'private domain'. The court noted that analysis of 'private domain' is contextual and changing, and analysed privacy theories proposed by Israeli privacy law scholars Gavison[38] and Birnhack,[39] as well as Warren and Brandies' article, to consider whether—based on different theories of privacy—there could be privacy in public under section 2(3). The court found that Warren and Brandies' 'right to be let alone',[40] Gavison's 'right to prevent unwanted access', and Birnhack's 'right to control personal information' can all apply in what is in the ordinary sense a public place. Two additional points made by the court are pertinent to our discussion of Glass.

First, in determining what a 'private domain' is, the court considered the 'reasonable expectation of privacy' test enunciated by Harlan J in *Katz*.[41] After discussing the subjective element—namely that the victim had a subjective expectation of privacy—the court considered the objective element, the reasonableness. The court wrote:

> If intimate privacy of a couple is a value that society seems to protect, there is no material distinction between a clearing and an isolated car-park. In both cases, the efforts to be secluded are reasonable and ostensibly effective and society has an interest in protecting the secrecy of intimate conversation.[42]

The pertinent point, obvious from *Katz*, is that if a 'reasonable expectation of privacy' is protected, then an expectation of privacy is no longer protected when it is no longer reasonable. Obviously, expectations of privacy continually change with changing social norms and with evolving technology. Processes such as growing freedom of the press, gender equality, and the individualization of constitutional privacy rights, along with innovations from linotype machines and telegram to digital cameras and social networks continually shape and reshape privacy law. Glass and similar technologies could significantly contribute to this process, called 'erosion of privacy' in the popular press, and in legal terms more properly described as changes to what is 'reasonable' in expecting privacy.

Second, the court noted that photography is different from visual voyeurism or a fleeting glance. 'The couple cannot expect to be protected from random glances of this or that lone passerby, who chances upon the location despite its relative isolation. With that, they can certainly reasonably expect that they will not be filmed in that place.' Here the court noted that the 'reasonableness' of the expectation of privacy also goes to the medium of the violation. Where a passing glance of a couple making-out is insignificant, a video recording of the same is a violation of privacy. The court elaborated: 'Photography, even if the photograph is kept by the photographer with no intention of distribution, undermines entirely the autonomy of the object of the photograph. Crystallizing the image and the act—whether on digital media or on photographic paper—is an irreversible act of denial of privacy, which even when corrected (by destroying the record) is no longer in the hands of photographed person.'[43] Android devices already enable automatic uploading of photos as they are snapped. As compression and high-bandwidth technologies become ever better and more widespread, and as more users move to cloud storage, snaps will be copied and uploaded and perhaps shared in real-time; there will be no 'correction' of a photo taken in violation of another's privacy. A Swedish startup, Memoto, sells a tiny camera that attaches to the user's lapel; it takes a picture every thirty seconds, while activating GPS and other technologies to ensure precise location data. A user finishes every day with thousands of pictures from every interaction during the course of the day. No doubt there will soon be Glassware to do the exact same thing. Section 18(2)(5) of the Privacy Law provides a defence where privacy was invaded by photography in public and the victim was included randomly, coincidentally. But as Glassware starts taking pictures every few seconds, and where this includes a picture of a given victim, this may no longer constitute 'random' photography or 'coincidence'; the user has knowingly decided to chronicle with photos every (half) minute of his day. Aside from the feeling of perpetual surveillance discussed above, this has the effect of magnifying the harm from every fleeting glance, awkward moment, or embarrassing situation.

It is not just case law that dismisses the actionability of a passing glance. Section 6 of the Privacy Law makes *de minimis* invasions of privacy non-actionable. Under the header 'An Inconsequential Act' the law states in section 6: 'There will be no right to a civil or criminal suit pursuant to this law for a harm that is of no consequence' (my translation). There is a dissonance between the header and the language of the section; the header

38 Ruth Gavison, 'The Right to Privacy and Dignity' in Ann Swersky (ed.), *Human Rights in Israel: Articles in Memory of Judge Haman Shelah* (Yediot 1988) 61–80, 65.

39 Michael Birnhack, 'The Theoretical Underpinnings of the Right to Privacy' (2008) 11 *Mishpat uMimshal*, 11–75.

40 This formulation was not Warren and Brandeis', but Judge Thomas Cooley writing extra-judicially; see Warren and Brandeis (n 20), 195 n. 4.

41 *Katz v US* 389 US 347, 88 S. Ct. 507 (1967).

42 Para. 4(2)(b). My translation.

43 Para. D(2)(3).

speaks of an inconsequential act; the section speaks of inconsequential harm. However, it is uncontroversial in Israeli law that it is the language of the section that governs,[44] so it is inconsequential harm that is not actionable; therefore, even though having a camera attached to one's shirt clicking away all day may be an inconsequential act, the resulting harm may be truly consequential.[45]

Legislators in many jurisdictions have addressed the confluence of photography and smartphones and their potential to cause material harm. In particular this is the case in voyeurism. US Federal Law prohibits filming a person's private body parts.[46] Historically, still and video cameras were ordinarily too big to be used surreptitiously in everyday situations. However, with the advent of the smartphone, upskirting and downblousing became possible and many jurisdictions have responded with laws specifically outlawing such surreptitious voyeurism.[47] For example, Hawaiian state law criminalizes activity by a person who: 'Covertly records or broadcasts an image of another person's intimate area underneath clothing, by use of any device, and that image is taken while that person is in a public place and without that person's consent.' Israeli law has no need for this provision, since section 2(3) of the Privacy Law has been interpreted, as above, to apply even in a public place. But note the language of the Hawaiian provision above; merely observing another's 'intimate area' underneath clothing in a public place is not outlawed. It is offensive to women to have their bodies and underwear looked at, but if that same glimpse is recorded, then it is no longer a *de minimis* glimpse, it is criminal voyeurism. Israeli law goes further still by not requiring such a recording to be 'covert'; all the same, Glass may well meet this 'covert' criterion anyway. Google has said that the Glass camera cannot be activated without the screen activating, which is visible to others. This is scant protection indeed; the screen is only barely noticeable, and presumably future generations of the yet-to-be-released product will be smaller still and even less noticeable. Moreover, according to news reports, developers have already managed to get a wink to substitute for a more overt gesture to take a picture,[48] and even Google has produced a version of Glass that can be operated by winks.[49]

In summary, Glass and similar technologies will considerably change the 'reasonable expectation of privacy' and will thus dilute the availability of the Privacy Law's protection. They also alter irreversibly the treatment of inadvertent, passing, and hereto *de minimis* violations of privacy. The courts and legislators will have to respond to these changes and amend Israel's privacy law accordingly.

Eavesdropping

Section 2(2) of the Privacy Law makes unlawful eavesdropping a crime and tort of invasion of privacy—in addition to being a violation of the Eavesdropping Law. The Eavesdropping Law prohibits listening to, recording or copying another's conversation using a device, and prohibits placing or installing a device for that purpose (section 2(c)).

Glass has a microphone and can record and store—locally or in the cloud, such as Google Drive—sound, much as a smartphone can. However, as discussed above regarding visual privacy, since Glass is subtle, wearable, online, and integrated with the suite of Google services, it poses some unique challenges to privacy law, including with respect to eavesdropping. These challenges are considered presently.

First, a fear reflected in regulator and legislator correspondence with Google, discussed below, is that Glass can be used for surreptitious recording. Under Israeli law that may be a concern, but it is limited by the fact that eavesdropping is only outlawed if none of the parties to the conversation has consented, so recording one's own conversation is obviously outside the rubric of eavesdropping. Section 8(c) allows random, good faith eavesdropping in public; but that is only if the eavesdropping was in the course of recording material to be published or for research. It must also be *geluya*, meaning overt or visible. Glass is probably small enough to be considered covert; one has to know what it is, and be looking at the right-hand side of the person wearing it to understand

44 Criminal Appeal 317/63 *Zur v Attorney General* PD18 p. 95 per Kahan J; see also Aharon Barak—former president of the Supreme Court, writing extra-judicially: 'Interpretation in Law: Volume II—Statutory Interpretation' (1993 Nevo) 316–21, since affirmed by the Supreme Court in Additional Criminal Appeal 8613/96 *Jabarin v State of Israel* PD 54(5)193, 203 per Or J.

45 The Supreme Court has clarified that though a Privacy Law action cannot be brought for *de minimis* damage, a constitutional action may, ie a law causing even *de minimis* invasion of privacy may be struck down. See SCJ 8070/98 *Israeli Association for Citizen's Rights v Ministry of Interior* PD 58(4) 842, and discussion in Tene (n 30).

46 Video Voyeurism Prevention Act of 2004, 18 U.S.C.A. sect. 1801.

47 Des Butler, Sally Kift, and Marilyn Campbell, 'Cyber Bullying in Schools and the Law' (2009) 16(1) Murdoch University Electronic Journal of Law 84–114, 94.

48 Steve Henn, 'Clever Hacks give Google Glass many unintended powers' (*All Tech Considered* blog, 17 July 2013) <http://www.npr.org/blogs/alltechconsidered/2013/07/17/202725167/clever-hacks-give-google-glass-many-unintended-powers> accessed December 15, 2013.

49 Jordan Crook, 'The Google Glass Wink Feature is Real' (*Techcrunch* 9 May 2013) <http://techcrunch.com/2013/05/09/the-google-glass-wink-feature-is-real/> accessed December 15, 2013.

that this is a recording device. Also, future versions of Glass are likely to become smaller and more subtle. One need not even touch the device to activate the recording; one simply says 'OK Glass, start recording' or words to that effect. As discussed below, Google has patented a technique for activating Glass with neither words nor touch, but based on eye movements. Google says that 'One important feature is that Glass requires user commands to take a photo or record video—actions that also cause the Glass screen to activate, which is visible to others. . . . We also prohibit developers from disabling the display when using the camera.'[50] This apparently is meant to allay the fear that Glass can be used for covert recording. But though some form of control is currently required to activate the camera, that does not preclude it from being 'covert', especially as that control can be very subtle indeed. In addition, there appears to be no external indication that the microphone is active.

But a greater issue that Israeli law must contend with is the boundaries of 'eavesdropping'. In a class-action lawsuit currently in process, *In Re Google Inc. Gmail Litigation*,[51] the claimants claim that Google's Gmail service violates Federal and State Wiretap laws, and the California Invasion of Privacy Act (CIPA). For the present purposes one point is most relevant. Regarding the CIPA claim, Google refers to a previous case, *Diamond v Google Inc.*[52] in which the court

> dismissed the Section 632 claim because the plaintiff had not explained 'how Google could have possibly "overheard" the emails "by means of any electronic amplifying or recording device"' for purposes of the statute. The court also held that Section 631 cannot be expanded beyond its express limitations to telephone and telegraph equipment. . . . In particular, Section 632 is targeted at '[e]avesdropping.' See Cal. Penal Code § 632. Obviously, one cannot 'eavesdrop' on an email or other purely electronic communication in any normal sense of the word. *See Black's Law Dictionary*, 588 (9th ed. 2009) (defining 'eavesdropping' as '[t]he act of secretly listening to the private conversation of others without their consent.'). While Section 632 also refers to the 'record[ing]' of confidential communications, that reference must be interpreted consistently with the overall statute, which plainly focuses on oral communications.

In other jurisdictions eavesdropping may be limited to oral communications, but in Israeli law the definition of 'eavesdropping' is considerably broader. The Eavesdropping Law offers a broad definition of 'conversation', so as to include, *inter alia* not only phone calls, but also fax, telex, teleprinter, and inter-computer communications.[53] The Israeli Supreme Court has a history of purposive interpretation of statute, and will tend to interpret statute in its most modern meaning, such that it can best address technological change.[54] The Supreme Court has cited approvingly the Privacy Law's pre-legislative commission thus: 'The broadening of mass communication media, the development and growth of the spread of technological devices that enable eavesdropping, trailing and spying from afar, the increased collection and concentration of data by public and private elements . . . all lead to an escalation in the violation of privacy.'[55] The courts are aware that the technological development is a central reason for the Privacy Law, and the Privacy Law must be interpreted, to the greatest extent possible, such that it covers technological innovations. In line with the purposive interpretive trend among Israeli courts, and as noted by Birnhack, Israeli courts do in fact tend to find ways to apply the existing statute to novel technologies.[56]

Glass is distinguished by many technologies it already incorporates, and others that are known to be in the works. There already exist voice analysis apps that can analyse voices to determine mood, attitude, and personality. These have so far been used to monitor the user's mood, since that is generally what they hear, and for the most part they compare voice clips over time. However, with Glass these same apps could be used to monitor other people's mood. Glass has a unique combination of audio, camera, and eye-tracking. It is only a matter of time before it incorporates such sensors as a pulse monitor. Google has already been issued a patent for a technology that will give a user an indication of the direction and intensity of sounds,[57] and 'a speech-to-text feature determining text of the speech; and causing the wearable computing system to display the text of the speech.' This suggests that eventually one could eavesdrop without recording a conversation. One's Glass will provide a text, live, of a conversation happening out of earshot. Google is already a leader in speech-controls for computing and has added voice-control and voice-based activity to its products.[58] Google's new Moto X phone,

50 Google response to Congressional Bipartisan Privacy Caucus, discussed in the section 'The Glass Ceiling—Regulators React'.

51 <http://www.consumerwatchdog.org/resources/googlemotion061313.pdf> accessed December 15, 2013.

52 CIV-1202715, Marin County Superior Court.

53 Eavesdropping Law, section 1.

54 See at length Barak (n 44) at 132–3.

55 DN 9/83 *Military Court of Appeals v Vaknin* PD 42(3) 837, 852. For discussion, see A Schreiber, 'Privacy: Proprietary or Human Right? An Israeli Law Perspective' (2009) 1 Intellectual Property Quarterly 99–138, 106 n. 24.

56 Birnhack (n 23)

57 US Patent 8,183,997, issued 22 May 2012.

launched in August 2013, is in perpetual listening mode and activates the personal assistant when the owner says 'OK Google Now . . .',[59] much as Glass is activated by 'OK Glass'. The Eavesdropping Law has not yet had to contend with such technologies, but it will.

Israeli courts have faced similar challenges before. For example, the courts have addressed whether reading emails held on an ISP server is 'eavesdropping',[60] which in particular turned on the question of whether data packets are 'static' or moving as they make their way from my outbox to your inbox. Curiously, even that question was resolved by the court by comparing the packets to a 'car driving from Tel-Aviv to Haifa and on its way stops at a petrol station, can it be said that that stop breaks-up the journey of a person driving from Tel-Aviv to Haifa? Can it be said that the stop at the petrol station means the end of that journey and beginning of a new one?'[61] The court concluded that it cannot, and therefore ruled that the communication is in transit, such that accessing it requires a wiretap permit, and not a regular search permit.

Courts have specifically addressed technological changes and the resulting social changes. In one case an employee borrowed his supervisor's cell phone under the guise that he'd forgotten his and needed to make a call. The employee gave it to a colleague who copied all the files of the phone, including voice recordings which the employees later submitted in evidence in a case against the employer. The evidence was not allowed since it was obtained by invasion of privacy.[62] The court noted:

> Smart mobile phones that are used by many of the public these days contain a lot of private information, including also photographs, messages, emails and so on. Anyone who asks to use another's phone must know this, and knows it. It is certain that the fact that a person lent their phone to another to use (for a phone call, sending a message or any other use) does not imply permission to the borrower to penetrate the phone and search it for information he needs.[63]

The court here demonstrated a much-needed awareness not only of technological change, but of the behavioural change that goes with it. In order to address the digital revolution, the Eavesdropping Law was amended in 1995 to extend to communication between computers. Legislators or courts will similarly need to consider whether and how they apply eavesdropping law to Glass, particularly with new eavesdropping paradigms such as speech-to-text technology already patented by Google.[64]

The Glass ceiling—regulators react

Beyond the specifics of Glass and privacy law, Glass has set something of a precedent for regulatory and legislative interaction with industry around a potentially privacy-unfriendly product. Specifically, many Data Protection Authorities (DPAs) and the US Congressional Bi-Partisan Privacy Caucus have published public letters and have enjoyed public responses from Google, on the subject of Glass and the privacy concerns it raises. The tone, language, demands, and requests included in these letters are inconsistent with the authority of these institutions and with what can reasonably be expected from Google in light of the current state of the law in Israel and elsewhere. As DPA power grows, and as wearable computers and other such technologies and products come to market, DPAs must respond responsibly and appropriately in order to be effective.

In June 2013, the heads of data protection authorities of several jurisdictions, including *inter alia* the head of the Israeli Law, Information and Technology Authority—who is also the Database Registrar and Israel's DPA—and the chairman of the Article 29 Working Party, on behalf of its members, wrote Google CEO Larry Page a letter (the 'DPAs' Letter') requesting clarification on several privacy implications of Glass.[65] The gist of the letter was to emphasize that Google had not consulted any national Data Protection agencies throughout the design and development of Glass, nor kept them informed. The short letter gives the impression that the DPAs were practically offended by Google's failure to consult them in the process of designing Glass:

> To date, however, most of the data protection authorities listed below have not been approached by your company to discuss any of these issues in detail.

And again:

> To date, what information we have about Google Glass, how it operates, how it could be used, and how Google might

58 Christopher Mims 'Google is preparing for screenless computers' (*Quartz*, 15 August 2013) <http://qz.com/115304/google-is-preparing-for-screenless-computers/#!> accessed December 15, 2013.

59 <http://www.cbc.ca/news/technology/story/2013/08/12/f-moto-x-google-phone-review-nowak.html>.

60 For a history, see Criminal File (District, Tel Aviv) *State of Israel v Eliezer Philosoph* per Khaled J.

61 Ibid., para. 8(a)(5).

62 *Jubani* (n 23) para. 9.

63 *Jubani*, (n 23) para. 12.

64 One recent District Court case concerned cameras secretly installed in an office and found that that constituted eavesdropping, though from the ruling it seems the cameras did not record sound; Other Appeal (Beersheba District) 19094–02–11 *State of Israel v Yifrah et al.*

65 <http://www.privacy.org.nz/assets/Files/Media-Releases/Letter-to-Google-from-data-protection-and-privacy-officers-re-Google-glass-June-2013.pdf> accessed December 15, 2013.

> make use of the data collected via Glass largely comes from media reports, which contain a great deal of speculation . . ..

This approach in itself is not helpful. Google is under no obligation to consult the DPAs while developing Glass. Nor is Google under any obligation to inform the DPAs of its product features and design. Privacy by Design has taken off as a best practice for companies that profess to protect privacy, but even that framework does not necessitate interaction with DPAs.[66]

Here we may digress briefly to consider models which DPAs could use to regulate hardware and software that may infringe privacy. Peter Hustinx, EU Data Protection Supervisor, has publically explored the role of DPAs.[67] According to Hustinx, in the 1980s DPAs' main role was in influencing legislation, but with Dir 46/95/EC the DPAs' compliance and independent supervisory functions came into focus—as reflected both by the preamble and provisions of the directive, and by other instruments such as the European Charter of Fundamental Rights which, in article 8, recognizes protection of personal data as a fundamental right and provides for control by an independent authority. In EU law, DPAs are thus principally in a compliance role, and fulfil that role independently. He noted several alternate models available to the DPAs, including use of criminal law and administrative law to enforce DP regulation.

When considering the role of the Israeli DPA and privacy-infringing technology and products, several alternate models, each with some degree of precedent in other areas, are possible. First, note that in Israel, as in the EU and elsewhere, a product that is designed to infringe privacy is not unlawful, nor are there any product-specific guidelines. One avenue is therefore to establish a regulatory framework with which a product must conform. An example is section 11 of the Eavesdropping Law which gives the Prime Minister, with a Knesset subcommittee, the power to regulate 'whether by licensing or otherwise, the production, sale, import, distribution and possession of devices which may be used for eavesdropping or types of such devices'. The Privacy Law has no parallel to this provision, and so the DPA has no power to regulate privacy-infringing devices. Following the Eavesdropping precedent, the DPA could be granted the power to regulate privacy infringing products.

However, although at a doctrinal level that may be appropriate, in Israel, as in many jurisdictions, the DPA is woefully under-resourced and over-extended.[68] This would add a considerable burden to an already stretched authority. Moreover, the pace of change of technology is such that the DPA would have to grow and train its team of investigators constantly in order to ensure it is capable of understanding and analysing emerging technologies. In other words, the burden would increase considerably over time. The Israeli DPA—like most, presumably—is not organizationally prepared for such a mission, or capable even of acquiring the capabilities to handle it, at this time.

A course less onerous to the regulator and less impractical would be to determine general standards and principles, presumably based on the Privacy Law, which would form the backbone of an industry standard. The regulation would be managed not by the DPA, but by a quasi-governmental body. This is the norm for all goods in Israel regarding quality standards, including safety. Pursuant to the Standards Law 1953, all product manufactured in Israel must meet the standards set by the Standards Institution of Israel (SII), a body created by the Standards Law and subject to the oversight of the State Comptroller. However, several factors militate against such a route. First, the law is slowly evolving away from pre-approval and oversight of this kind, and the Knesset recently approved the second reading of the Standards Law (10th amendment) 2013 which specifies areas in which imports may be made of goods that have various international certification, or for which the importer has made certain declarations, all considerably less onerous than going through the SII process. Second, in contrast with technical standards, invasion of privacy is generally much harder to evaluate, and there is almost never a device that is employed exclusively for the invasion of privacy. Here copyright poses a useful comparison: there have been a handful of cases regarding attempts at stopping the distribution of double-deck cassette recorders, photocopy machines and other technologies that help infringe copyright; though some cases had success, in the long run they mostly failed—the *Napster* cases are an instructive exception—and these technologies spread because they enabled but did not authorize copying,[69] or because they have other, non-infringing uses.[70] Technologies that infringe, or may infringe, on privacy rights are everywhere; GPS devices, cameras, microphones, voice-recognition software, facial recognition software, and more are all so trite that every

66 <http://www.privacybydesign.ca/> accessed December 15, 2013.

67 Peter Hustinx 'The Role of Data Protection Authorities' in Serge Gutwirth et al (eds) "Reinventing Data Protection" (Springer 2009) pp.131–7.

68 Christopher Kuner, 'Transborder Data Flows and Data Privacy Law' (Oxford University Press 2013) 144.

69 *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1987] 2 WLR 1191 (HL).

70 *Sony Corp. of America v Universal City Studios*, 464 U.S. 417 (1984).

smartphone includes them all, and yet barring some highly specialized spying equipment none of it is designed to invade privacy *per se*. In short, not only are privacy-violating devices (outside of eavesdropping) not generally unlawful or regulated, it would be very difficult to regulate them irrespective of the difficulties of enforcement; either the net would be cast so wide as to include non-infringing devices or devices with alternate uses, or it would be so narrow as to be worthless.

Perhaps the greatest reason to avoid DPA discretion to regulate privacy-infringing devices is that both freedom of speech and privacy are constitutionally protected rights in Israel (as in most liberal jurisdictions).[71] The balancing of these major societal values and legal principles is best done by supreme courts, and occasionally by the legislature, and not by a regulator or a quasi-governmental authority. They could give the DPA clear guidelines to implement and the resources to do so, but the high-level, delicate balancing of conflicting values is not what DPAs are expert at and should not be within their mandate.

A more workable course would be private-sector solutions. Bennet and Raab have coined this 'self-regulation of privacy', and give examples of industry-determined standards and codes of practice.[72] Products could be subjected to third-party privacy audits and have some privacy seal of approval, much as sites may have TRUSTe or some similar certification.[73] This could be layered—with different standards and certifications available for hardware, operating systems, applications, and so on. Privacy by Design originated with a DPA and enjoys widespread support from DPAs, including the Israeli DPA as noted below. But its implementation is probably best left to the private sector. Data protection and privacy standards and best-practices may be initiated in academia or by regulators, but are probably best established, supervised, and enforced by market forces.

Leaving the normative and returning to our examination of the DPA Letter, it is evident that the Israeli DPA was making demands out of line with its authority, and beyond its enforcement powers. Israel's Privacy Law includes both chapter 1—relating to invasions of privacy generally, and chapter 2—relating to databases. The DPA's role was established thus in section 10 of the Privacy Law: 'The Registrar shall supervise the compliance with the provisions of this Law and the regulations thereunder.'[74] Israel's DPA could apply a broad interpretation to this provision in order to somehow exercise veto rights over consumer products that may invade privacy. This would be a draconian move that would rightly meet with extreme resistance in Israel, and would also be a dramatic reinterpretation of the powers of the DPA. Such an interpretation is not inconceivable, particularly given the Supreme Court jurisprudence pursuant to which protection of privacy under the Basic Law: Human Dignity and Liberty may be broader than under the Privacy Law alone, and extends to protection of data in databases—chapter 2 of the law.[75] But beyond the question of the DPA's authority, it is clear that this would be beyond the DPA's capability since the enforcement powers specified in subsequent provisions all relate to databases: 'The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order, a supervisory unit that *will supervise the databases*. . . . In carrying out his functions, an inspector may—(1) demand every relevant person to deliver to him information and documents *relating to a database*; (2) enter a place as to which he has reasonable belief that *a database* is being operated, search the place and seize objects . . .'[76] In other words, although the registrar, Israel's DPA, is technically charged with ensuring compliance with the entire Privacy Law, the DPA's enforcement powers are all limited to databases. Regarding a database, the Registrar can use section 10(a)(2) to make various demands. For example, Google Street View was determined to constitute a database under section 7 of the Privacy Law, and Google submitted a request for registration. On 21 August 2011, the Registrar allowed[77] the registration subject to a list of conditions, the last of which was that Google will commit to apply Privacy by Design principles, and will act judiciously to blur identifying features (eg faces) and keep un-anonymized data for the minimum possible time. These are pretty broad demands and could only be made in connection with registering a database. But that is not the case with Glass, which involves no database, making both the content and tone of the DPAs—at least vis-à-vis the Israeli DPA—misguided. Thus for the Israeli DPA, the DPAs' Letter is all bark without so much as the capacity to bite.

71 Privacy is protected in Basic Law: Human Dignity and Liberty, sect. 7; freedom of speech is not expressly protected in a Basic Law, but is in the Israeli Declaration of Independence, and in a string of Israeli Supreme Court cases. See SCJ 73/53 *Kol Haam Ltd v Minister of Interior* PD7(2) 871.

72 Colin J Bennett and Charles Raab, 'The Governance of Privacy: Policy Instruments in Global Perspective' (MIT Press 2006), ch. 6.

73 European Data Protection Supervisor, Peter Hustinx, 'The Role of Data Protection Authorities', in S Gutwirth, Y Poullet, P Hert, C Terwangne, and S Nouwt (eds), 'Reinventing Data Protection?' (Springer 2009) 131–7, 137.

74 Sect. 10, Privacy Law.

75 SCJ 8070/98 *The Association for Civil Rights in Israel v Ministry of Interior*PD 58(4) 842, 853 (2004). See discussion in Tene (n 30) at 68–69.

76 Ibid sect. 10(d)–(e1), emphasis added. The same applies in sections 10(f), and 11.

77 <http://index.justice.gov.il/Units/ilita/PressReleases/21811.pdf> accessed December 15, 2013.

The DPAs' Letter then goes on to list several queries, a couple of which demonstrate just how perplexed the DPAs are with respect to Glass and their role. The first question is: 'How does Google Glass comply with data protection laws?' This question almost defies belief; it purports to shift the burden of proving legality from the DPAs to Google, as if Google is required to get DPA approval for a product release. Another notable question is: 'Would Google be willing to demonstrate the device to our offices and allow any interested data protection authorities to test it?' This is worded as an inquiry. If the DPAs believe they have the power to demand to test the product, they could exercise that power. If they want to test Glass in order to learn about the new technology, they could make the request of Google but that should not come in a letter from multiple DPAs implicitly claiming that Glass is not lawful. The DPAs are implying that Glass is illegal on the one hand, and meekly requesting to play with Glass on the other; the messages are so mixed that Google's evasive response was inevitable.

An additional point is worthy of consideration. The reason for the DPAs' election to make their letter public is not clear. In contrast with the Congressional Privacy Caucus, discussed below, the DPAs have authority over Google in respect of many of its activities in many jurisdictions. In so far as the requests made in such a letter are within the normal authority of each DPA, they should have been addressed to the relevant entity in each jurisdiction. Taken with the points above, one cannot escape the impression that the DPAs were joining the mass of concerned voices in the blogosphere and in talkbacks and commentary. The letter is altogether unprofessional and will not encourage Google or other such companies to voluntarily engage with DPAs in the future.

Predictably, Google's response of 22 July 2013[78] does not directly address a single one of the questions in the DPAs' Letter. Google's Global Privacy Counsel, Peter Fleischer, noted in the letter that Google had been 'designing Glass with privacy in mind' and that the product has not launched yet and Google continues to learn from the feedback it receives. Other specific details of how Glass' camera is operated for example, are basically repeats of Google's response to a previous letter it received in April 2013, and are discussed presently.

In April 2013 the members of the US Congressional Bipartisan Privacy Caucus wrote publically to Google CEO Larry Page asking for several clarifications on the expected impact of Glass on privacy.[79] The letter states:

> As members of the Congressional Bi-Partisan Privacy Caucus, we are curious whether this new technology could infringe on the privacy of the average American.

On that premise, the letter continues to list several questions regarding potential breaches of privacy that can be affected with Glass. The statement of the premise for this letter is very poorly worded indeed. No doubt the members are more 'concerned' than 'curious', but a more important point is that the technology can obviously infringe on, or facilitate the infringement of, the privacy of the average American. The same is true of many of the most ubiquitous technologies in our world today, from smartphones and digital cameras to Gmail and GPS, and obviously so for Glass which includes all of those elements. The concern that both the bipartisan caucus and the DPAs failed to voice is that this device is largely optimized for breaching privacy. Glass is designed to integrate seamlessly and unobtrusively with, and participate in, our everyday activities. It hears our conversations, sees what we see, goes where we go and all the while interacts with our email, location, calendar, contacts, navigation and so on. This is a significant step up from smartphones. Google CEO Larry Page reportedly said that 'Obviously, there are cameras everywhere. People worry about all sorts of things that actually, when we use the product, it is not found to be that big a concern. You don't collapse in terror that someone might be using Glass in the bathroom just the same as you don't collapse in terror when someone comes in with a smartphone that might take a picture. It's not that big a deal.'[80] One of several pertinent differences between smartphones and Glass—and no doubt Page is more than aware of these—is the potential Glass has to wreak havoc on privacy. Google's response[81] to the Congressional Caucus letter focuses principally on the privacy of Glass users, but also makes some remarks, discussed below, regarding protection of the privacy of those around the Glass user mostly noting that Glass' camera cannot be operated covertly. For example, one touches the device or speaks to it in order to operate the camera and that also activates the screen, which is visible.

Again, Google's responses to the DPAs and to the caucus contribute to our understanding of how Google

78 <http://oaic.gov.au/images/documents/Letter_to_Privacy_and_Data_Protection_Commissioners_from_Google_June_2013.pdf> accessed December 15, 2013.

79 <https://joebarton.house.gov/images/user_images/gt/GoogleGlass Ltr_051613.pdf> accessed December 15, 2013.

80 Liat Clark, 'Global data privacy leaders: let us play with Google Glass' (Wired.co.uk 19 June 2013) <http://www.wired.co.uk/news/archive/2013-06/19/google-glass-privacy-notice> accessed December 15, 2013.

81 <http://joebarton.house.gov/images/user_images/gt/Google_Glass_Response_2013_Letter.pdf> accessed December 15, 2013.

views Glass' impact on privacy, and co-chair of the Congressional Caucus Representative Joe Barton (R-TX) said so in his public response to Google's reply: 'I am disappointed in the responses we received from Google. There were questions that were not adequately answered and some not answered at all.'[82] But other sources offer considerable insight. In May 2013 Google applied for a patent whereby Glass can be controlled by eye movements—specifically to unlock or activate Glass, presumably without the need for saying 'OK, Glass'. That basically undoes the central claim of Google's response—that the camera is operated by a visible touch or an audible instruction. In other words, Google claimed that the camera cannot be activated covertly, but has just filed a patent for allowing covert activation of Glass.

More importantly perhaps, in August 2013 Google was issued a gaze-tracking patent.[83] Google's patent is very specific on some of the future functions of Glass. Here are some highlights from the claims of this issued patent:

- "A method comprising: receiving scene images from a head mounted gaze tracking device capturing external scenes viewed by a user wearing the head mounted device
- receiving gaze direction information . . . indicating where in the external scenes the user was gazing when viewing the external scenes
- image recognition algorithm on the scene images to identify items within the external scenes viewed by the user;
- generating a gazing log tracking the identified items viewed by the user;
- performing latent pre-searches on at least a portion of the items viewed by the user
- indication of whether the user looked directly at the identified items
- charging advertisers associated with the advertisements based at least in part on a per gaze basis . . . [and] the tendency of a given advertisement to draw user gazes or to hold the user gazes . . . [and] the tendency of a given advertisement to evoke an emotional response
- inferring an emotional state of the user while viewing the external scenes based at least in part upon the pupil dilation information; and storing an emotional state indication associated with one or more of the identified items"

Note the last two bullet points: Google has patented a system for inferring the user's emotional state based on pupil dilation. It has also patented a method for charging advertisers based on that emotional state. This highlights additional privacy concerns, beyond the rubric of this article, that Glass will introduce: in addition to Google and others having knowledge of one's location and destination, activity, finances, schedule, and so on, it will now know one's emotional state. This will have bearings on third parties that we cannot contemplate yet, but those are sure to be interesting and challenging. That regulators and legislators are concerned is good, but they must be more deliberate and thoughtful if they are to communicate effectively and collaborate with industry to address emerging technologies.

Conclusion

Wearable computers, led by Google Glass, will both challenge and shape privacy law in the coming years. Current legal provisions are not best suited to protecting privacy from the proliferation of Glass and wearable computers. A near-constant feeling of being observed, coupled with a technology that can record in video almost all activity going on around a person, converge to alter the way privacy may be enjoyed and protected. Reasonable expectations of privacy are changing, as well as the potential for harm from what used to be *de minimis* invasions of privacy.

Glass and its adjacent technologies such as speech-to-text and gaze-tracking, will challenge the legal definitions of eavesdropping and conversation, and of what is 'covert', for example, and will necessitate reconsideration of the parameters of privacy and eavesdropping laws.

DPAs must develop a policy on interaction with industry regarding potentially privacy-infringing hardware and software. In all likelihood, a private-sector solution, establishing best-practices, audits, and seals of approval will be most effective. The extent to which, if at all, DPAs ought to be consulted in product design, for example, should be the subject of public debate and of deliberate legislation. Glass has perplexed DPAs and in this may quickly bring into focus the need for DPAs to be more thoughtful and deliberate. Hopefully in this regard Glass will have a strong positive influence on privacy law, by catalysing a considered reevaluation of the DPAs' role and authority.

doi:10.1093/idpl/ipt034

82 <http://joebarton.house.gov/press-releasescolumns/barton-disappointed-by-response-to-google-glass-privacy-concerns/> accessed December 15, 2013.

83 US Patent 8,510,166, 'Gaze Tracking System', issued 13 August 2013.