The introduction of 'voluntary' microchip technology in the workplace: an innovative solution or invasion of privacy?

Ysabel Jana Dela Rosa

University of Bath
Tutor: Professor Andrew Crane

Winner: Postgraduate Category
Institute of Business Ethics Student Essay Competition 2019

Executive Summary

The essay evaluates whether the decision of Three Square Market, a US-based technology company, to introduce microchip implantations to their employees was an ethically correct decision. This was written to investigate the appropriateness of applying new and emerging technologies within a corporate-and potentially commercial- setting. Using the principle of the UN Declaration of Human Rights, particularly Article 12 which focuses on issues of privacy and surveillance, Part One provides a contextual overview of the factors which led to the company's decision to innovate the use of RFID technology within the US, whilst Part Two applies Hohfeld's theory of moral rights and duties to critically discuss the ethical implications of this corporate decision. Ultimately, whilst emphasis has been placed upon the voluntary nature in which employees continue to acquire microchip implantations, and that this technology has been approved by the US Food and Drug Administration in 2004, Three Square Market was still found to garner human rights offences against the protection of employee privacy within and outside the workplace. It is recommended that national institutions restrict the use and further release of this technology until sufficient data has been conducted to measure its long-term implications.

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk

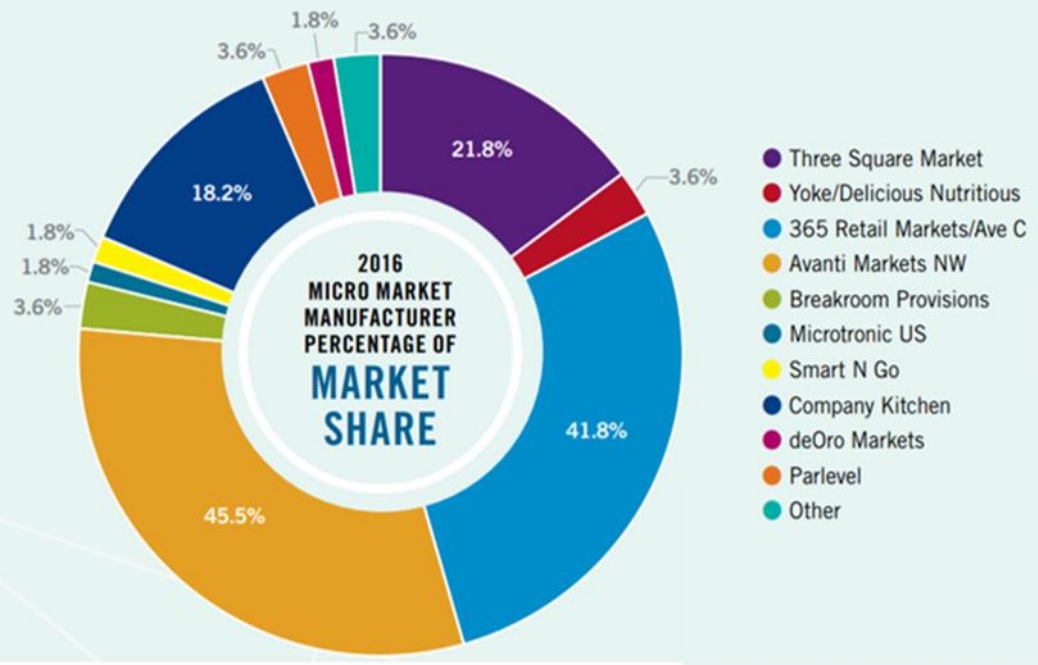
Registered Company No. 11594672
Registered Charity No. 1180741

On August 1st 2017, a U.S. micro market technology company- Three Square Market (32M) - introduced voluntary microchip (RFID) implantations to employees, giving them the opportunity to replace standard access cards, passwords and credit cards. They are the first U.S. company to propose this (Gillies, 2017; Cox, 2017), and as of August 2018, 48% of employees opted to be microchipped. 32M predicts this to rise given the public's increasing global exposure to wearable technology, and the emergence of "implantables, embeddables and even ingestibles" (CNBC, 2018; Thierer, 2015:31). While this use of the RFID chip technology was approved by the U.S. Food and Drug Administration (FDA) since 2004 (NBC News, 2004), 32M continues to receive criticism due to the human rights risks posed, such as the extent 32M opens employees to security and privacy risks given the developments with microchips, which includes GPS tracking, storage of financial and medical data etc. (Kurkovsky et al. 2010; Vander Wier, 2017; Kopplin and Platt, 2018). Using the Hohfeldian approach with a focus on its human rights implications, this essay discusses why it was ethically incorrect to introduce voluntary microchipping in the workplace.

Part One:

The CEO of 32M, Todd Westby, justified the use of microchipping with two factors: their competitive industry, and the inevitability of microchip technology for mainstream use. Firstly, in the U.S., micro market providers are a consistently growing industry since 2005, accounting for 12.9% ($2.8 billion) of sales revenue generated by the vending industry in 2015 (Refermat, 2016.) However, with this growth, the number of competitors in this market is only expected to rise; micro market companies perceived this as a prominent challenge in 2016 (Refermat, 2017.) As seen in Figure 1, whilst 32M secured 21.8% market share in 2016, becoming third in the U.S.' micro market industry, there was at least a 20% gap between 32M and the market share acquired by each of the top two market leaders. As mentioned in their website, 32M's mission was always to become "a global leader" (2018), therefore it is fair to state that they devised strategies to achieve this. As 32M's CEO states on their LinkedIn profile (Westby, 2018), "this microchip concept […] went viral and we have over 1.2 billion views along with 150+ interviews with different companies around the world." 32M benefited from countless national and international media coverage since it declared this decision, thus it can be argued microchipping employees was partly motivated by 32M's desire to secure market leadership by enhancing their business' global visibility.

Figure 1: U.S. micro market share in 2016 (Refermat, 2017)



24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk
Registered Company No. 11594672
Registered Charity No. 1180741

Moreover, market leadership can also be acquired through innovation. According to Refermat (2017; 2016), perceived market saturation in the micro market industry rose to 7.3% in 2016 from zero in 2015, with several operators opting to propose commissions and market accounts which are under minimum profit baselines to survive. As mentioned by Westby prior to the release of microchips, "it's the next thing that is inevitably going to happen, and we want to be a part of it" (KSTP TV, 2017.) And as 32M's COO, Patrick McMullan, stated (Cox, 2017), "this technology will become standardized […] the international marketplace is wide-open […] the future trajectory of total market share is going to be driven by who captures this arena first." This implies that 32M aimed to position themselves at the forefront of technological advancements using microchips to avoid falling prey to market saturation.

Additionally, as the chip enables employees to access the building, logon to devices, and purchase items from office stores, there are several articles which claim the decision to microchip was motivated by their desire to reduce workforce "friction" and make the lives of employees more convenient (Vander Wier, 2017; Kopplin and Platt, 2018.) However, a year after its release, it is important to note that Westby has spoken about 32M's ongoing development of "an actual chip that will be powered by the human body […] have GPS tracking capabilities along with voice recognition" to be released to the market (CNBC, 2018). Apart from streamlining the employees' daily operations, thus resulting to an increase to overall employee satisfaction (Lohrmann, 2017), there is a noticeable marketability with its usage. It is possible that 32M implemented this technology to investigate the strengths and limitations of existing RFID technology, to further develop its potential to either introduce this new device to the micro market industry or diversify their product range.

Part Two:

Initially proposed by Wesley Hohfeld (1919, as cited in Lazarev, 2005) as a means to determine rights and liberties under the philosophy of law, the Hohfeldian analysis has been a widely accepted framework for evaluating the delivery of human rights, given its emphasis on the correlative relationship between right and duty, and consideration of the consequences which arise from such rights and duties (Gewirth, 1984). Hohfeld's theory is rooted in the principle of correlative relationships, as seen in Figure 2. Hohfeld states that these incidents can only be matched with a specific other if one is to preserve the morality of rights, i.e: If person X has a *Claim* against person Y regarding a right, then person Y has the *Duty* to provide for this, yet if person X has *No-claim* for a certain right, then person Y has the *Liberty* to decide whether or not to provide this right. This theory states that all first-order rights, rights to which every individual is entitled to, can be categorized using this framework.

On the contrary, second-order rights can manipulate first-order rights, and these are dependent on the existing authorities, institutions and hierarchies which occur within a given context. Within the pairings of second-order rights, the correlatives which exists are *Power* with *Liability,* and *Immunity* with *Disability*. To put it simply, if person X has *Power* over person Y, then person Y is at *Liability* to follow the duties imposed by person X. However, if person Y is granted *Immunity* from these duties, then person X has *Disability* and must retract these imposed duties. Table 1 provides a summary of these terms.

Figure 2: Correlatives within Hohfeldian Analysis

First-order rights		Second-order rights	
Claim	Liberty	Power	Immunity
Duty	No-claim	Liability	Disability

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk
Registered Company No. 11594672
Registered Charity No. 1180741

Table 1: Dimensions of the Hohfeldian Analysis

Term	Definition
Claim	To have the right to enforce a duty upon another.
Duty	The obligation to perform an action based on a duty.
Liberty	The freedom to choose to perform an action based on a duty.
No-claim	To have no right to enforce a duty upon another.
Power	An individual's ability to alter moral pairings.
Liability	An individual's inability to alter moral pairings.
Immunity	An individual's protection from imposed duties.
Disability	An individual's inability to impose duties.

Under second-order rights, particularly with power and liability, it could be argued that because the CEO of 32M has the ultimate authority within the organizational scope of the company, his employees are at liability to follow the rules enforced, and therefore agree with the implementation of microchips. However, with immunity-disability correlative, this can also be said about the relationship between the company and external institutions, whereby 32M are at disability to US law, particularly in regards the US Supreme Court's ruling in 1954 about data protection; government authorities within the state can monitor the fair collection and storage of data by businesses and renounce operations which infringe upon this (Thoren-Peden and Meyer, 2018.) In this case, a purely legislative view of power and immunity nullifies each argument, therefore it is important to focus on the implications of first-order rights when reviewing human rights, as it enables a balanced consideration of both 32M and employees, stating that they have an equal claim or a liberty for a particular action.

According to first-order rights, claims enforce duties whilst the lack of claims enable liberties. As stated in Article 12 of the UN Declaration of Human rights (1948), "no one shall be subjected to the arbitrary interference with his privacy […]", therefore in relation to the claims of both 32M and employees, there they must remove microchip technology within the workplace if 32M is unable to protect their employees' right to privacy; either directly or indirectly. Recent studies have shown that there are uncertainties and risks posed by microchip technology, particularly in terms of its potential to infringe on personal privacy and security, thus making it a morally incorrect action to introduce to employees. Current RFID technology, like the one 32M uses, have the capacity to track the movement of a tagged entity and collect data surrounding its movement, storing information such as its location, patterns of behavior etc. (Kurkovsky et al., 2010.) This opens employees to threats of constant observation and surveillance in and outside of the workplace, given that these chips are implanted rather than a wearable item which can be removed, thus blurring the line of the scope to which 32M can survey the actions of their employees.

As stated by data privacy researcher Michelle de Mooy, companies "start off wanting data for one reason and end up using it for many others." (Fast Company, 2018.) This tendency to abuse boundaries is certainly noticeable within 32M. In an interview prior to the release of microchips, Westby mentioned that "there is no GPS tracking at all", nor do they plan to release this feature to their employees (Gillies, 2017.) However, in a recent interview with this CEO, he states that they are in development of an RFID chip which "will have GPS tracking capabilities along with voice recognition." (CNBC, 2018.) Whilst this is not directly inferred for use to employees, it does not refute the fact that such a technology exists, and employees have been misinformed of the capacity prior to implanting this chip; 32M stated that it was introduced solely for their convenience in the workplace. Furthermore, since its approval for human use by the FDA in 2004, implantable RFID microchips have been used in monitoring personnel in other fields, such as military and law enforcement officers to name a few (Kurkovsky et al., 2010.) This begs the question of whether the privacy of employees were protected in the first place if an identical technology has been in operation for more than a decade, with the purpose of tracking the individual's behavior. Tracking features are presently available, and given that 32M already pushed the boundaries with the capabilities of their microchips- from their initial statement of refusing GPS to presently developing this added feature- then what limits them from infusing this supposedly new feature upon the microchips implanted in employees?

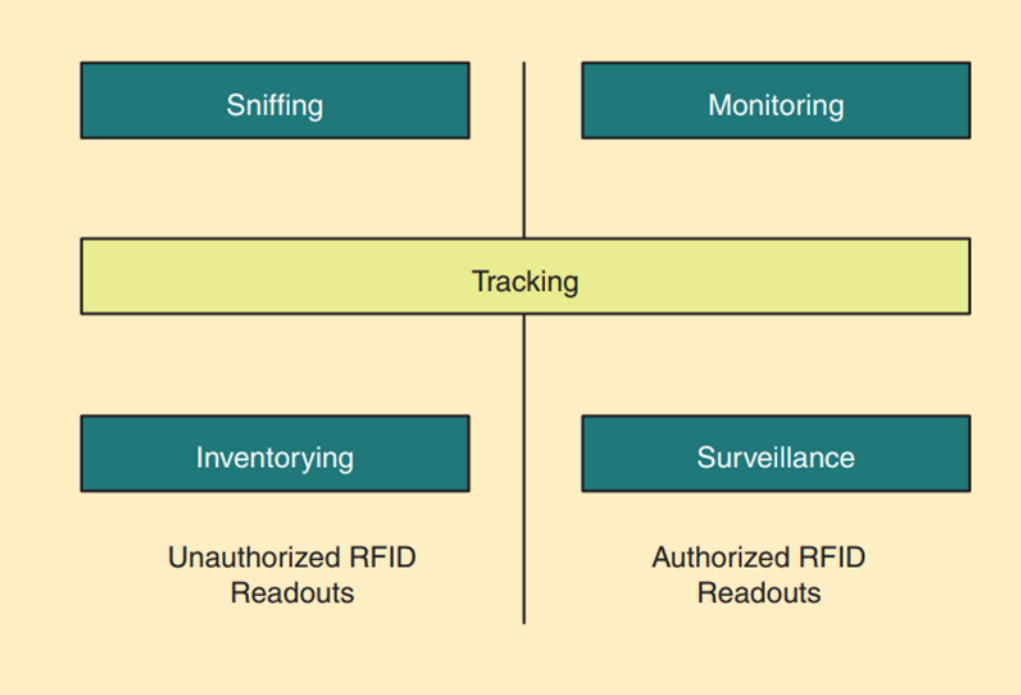
24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk
Registered Company No. 11594672
Registered Charity No. 1180741

One may also argue, based on no-claim and liberty, that there is no fundamental right to refute 32M's microchip technology because the device was granted FDA approval in 2004; therefore 32M has the freedom to choose whether or not to utilize this technology as they see fit. As defended by McMullan, "this is an approved device, there's been nothing that has come out since 2004 that has done anything to change the FDA's stance on it" (Fast Company, 2018.) However, this claim is invalid due to the misleading data provided to employees when they agreed upon this implant, and the context in which microchips are used. Firstly, in reference to the earlier point concerning microchip capabilities, these have always had the potential for tracking location, thus negating Westby's claim that "there is no GPS tracking at all"; a fact he has informed employees prior to implantation. This misleading information falsifies the argument for voluntary microchips, as employees did not knowingly volunteer to have the added feature of GPS tracking. And while one can still state that there is no conclusive information which confirms GPS tracking, the fact remains that the potential is there, thus exposing employees to "an arbitrary interference of privacy" (UN, 1948.) Secondly, it is important to bear in mind the context of the FDA's approval. Their decision to allow for the national use of human microchip implants was to track and store patient records, particularly in case of the patient being unresponsive or have undergone countless treatments (NBC News, 2004.) This brings forth the issue of consent. For McMullan to argue that 32M has claim to an identical technology, and for identical usage, is invalid as its intention was rooted in medical practice, whereby those who provided this option to patients are legally obligated to be transparent with patients about the extent data will be stored and processed within their system. Therefore 32M cannot claim for the rights approved by the FDA given that their corporate application does not match the initial intention and application approved by the organization.

Furthermore, even if one is to argue that it cannot be proven 32M has misused sensitive employee data, or that they should be able to claim FDA approval rights given its widespread use in other sectors, this device still indirectly exposes employees to privacy breach from external parties. According to Kurkovsky et al. (2010), one of the main concerns with this technology is its inability to implement strong authentication and encryption barriers, thus leading to unauthorized RFID readouts and the leak of sensitive information. Figure 2 outlines how privacy is lost with RFID technology. The microchips are standardized therefore if employees are to be implanted, they must agree to all its present uses in 32M. One of the features of their implant is its ability to pay for items in the company's stores (Gillies, 2017), and this means that their bank details are stored within the chip. Privacy concerns are raised due to the technology's weak infrastructure, which makes it possible for malicious individuals to decode the encryption and acquire sensitive data as long as they are in possession of an RFID reader (Piramuthu, 2007.) Returning to Hohfeld's correlative incidents, if 32M is to claim a right for its deployment, then they also have the responsibility to ensure the security of the data stored, and that employees will not be subjected to the unauthorized collection of sensitive data, either internally or externally, because they exposed employees to this potential vulnerability. However, when asked about the privacy risks involved with external parties, McMullan responds with the following: "is anything hackable? That's a stupid word […] The thing that's in your hand has a 256-bit encrypted password […] its significantly harder to try to take anything off this." (Fast Company, 2018.) Ultimately, senior management representatives of the company have refused to accept the responsibility of maintaining privacy rights of employees, even going as far as indirectly shifting the blame of personal security breaches to the individual (CNBC, 2018.) Given that they are the ones to introduce this technology, they are responsible for protecting employee privacy. Since the device lacks the essential security measures, and 32M actively denies responsibilities for enforcing security measures, 32M fails to deliver the duty of privacy, thus making it an ethically wrong decision.

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk
Registered Company No. 11594672
Registered Charity No. 1180741

Figure 3: Loss of privacy with RFID technology (Kurkovsky et al., 2010)



In conclusion, the Hohfeldian analysis is a valid approach for evaluating this decision as it explores the rights entitled to all parties, and considers the reality that certain rights can be made invalid with the privilege and power of certain authorities. Though the basis of human rights are fundamentally claim-rights (Gewirth, 1984), it expands towards power and immunity correlatives when discussing its preservation within the broader social context. This theory acknowledges that both employees and 32M are entitled to first-order rights: the right to introduce new technologies, and the right to refuse new technologies. However, this theory also recognizes the existence of higher authorities and institutions external to 32M who govern moral and legal duties (i.e: the U.S. government, the U.S. F.D.A, and the UN) and have the power to invalidate claims of 32M. Ultimately, the benefit of applying the Hohfeldian analysis is that it considers the complex internal structure from which rights are constructed, provides a methodological approach in determining the entitlement of duties, and expands claims to include all authorities, thus enabling a consideration of the wider ethical implications of claims and liberties. Lastly, the fact that it remains optional is not a valid defense as it does not protect employees from privacy infringement once implanted, a key factor of human rights which 32M is accountable for given that they released this technology. And while it remains to be in the experimental stage of its usage, it continues to gather widespread interest, particularly with UK companies (Kollewe, 2018.) It is therefore more important to implement measures and institutions which will closely monitor the use of microchips in the workplace to maximize organizational benefits and minimize risk to human rights.

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk
Registered Company No. 11594672
Registered Charity No. 1180741

References

CNBC. (2018). *Three Square Market CEO on implanting employees with microchips*. [online] Available at: https://www.youtube.com/watch?v=M4QiaHzcdyM [Accessed 18 Nov. 2018].

Cox, J. (2017). *This tech company is becoming one of the first in the world to microchip employees*. [online] The Independent. Available at: https://www.independent.co.uk/news/business/news/us-tech-company-microchip-employees-first-three-square-market-wisconsin-a7856971.html [Accessed 19 Nov. 2018].

Fast Company. (2018). *The Day I Got Microchipped*. [online] Available at: https://www.youtube.com/watch?v=43XzI6__abE [Accessed 19 Nov. 2018].

Gewirth, A. (1984). The Epistemology of Human Rights. *Social Philosophy and Policy*, 1(2), pp.1-24

Gillies, T. (2017). *Why one business opted to implant employees with microchips, and most jumped at the chance*. [online] CNBC. Available at: https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html [Accessed 16 Nov. 2018].

Kollewe, J. (2018). *Alarm over talks to implant UK employees with microchips*. [online] The Guardian. Available at: https://www.theguardian.com/technology/2018/nov/11/alarm-over-talks-to-implant-uk-employees-with-microchips [Accessed 2 Dec. 2018].

Kopplin, K. E. and Platt, S. J. (2018) Wave of the future? Company offers to microchip employees, *HR Specialist: Texas Employment Law*, 13(1), p. 6

KSTP TV. (2017). *Wisconsin Company Three Square Market Becomes First In United States To Microchip Their Employees*. [online] Available at: https://www.youtube.com/watch?v=5I27upoq0zA [Accessed 16 Nov. 2018].

Kurkovsky, S., Syta, E. and Casano, B. (2010). Continuous RFID-enabled authentication and its privacy implications. *2010 IEEE International Symposium on Technology and Society*, pp.103-110.

Lazarev, N. (2005). *Hohfeld's Analysis of Rights: An Essential Approach to a Conceptual and Practical Understanding of the Nature of Rights*. [online] Available at: http://classic.austlii.edu.au/au/journals/MurUEJL/2005/9.html#n8 [Accessed 1 Dec. 2018].

Lohrmann, D. (2018). *Where Next for Microchip Implants?*. [online] Government Technology. Available at: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/where-next-for-microchip-implants.html [Accessed 5 Dec. 2018].

NBC News. (2004). *FDA approves computer chip for humans*. [online] Available at: http://www.nbcnews.com/id/6237364/ns/health-health_care/t/fda-approves-computer-chip-humans/#.WY4NoOvyuHs [Accessed 1 Dec. 2018].

Persson, A. and Hansson, S. (2003). Privacy at Work -- Ethical Criteria. *Journal of Business Ethics*, 43(1), pp.59-71.

Piramuthu, S. (2007). Protocols for RFID tag/reader authentication. *Decision Support Systems*, 43(3), pp.897-914.

Refermat, E. (2016). *Micro markets lift vending industry revenue to $20.9 billion*. [online] Available at: https://www.vendingmarketwatch.com/reports/document/12222476/2016-state-of-the-vending-industry-report [Accessed 19 Nov. 2018].

Refermat, E. (2017). *Operators Close 2016 With 7-Year High of $21.6 Billion* [online] Available at: https://www.vendingmarketwatch.com/management/article/12350375/2017-state-of-the-industry-operators-close-2016-with-7year-high-of-216-billion [Accessed 19 Nov. 2018].

Thierer, A. (2015). The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation. *Richmond Journal of Law and Technology*, 21(2), pp.1-118.

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk

Registered Company No. 11594672
Registered Charity No. 1180741

Thoren-Peden, D. and Meyer, C. (2018). *Data Protection 2018 | Laws and Regulations | USA*. [online] International Comparative Legal Guide. Available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [Accessed 1 Dec. 2018].

Three Square Market (2018). [online] Available at: https://www.32market.com/public/ [Accessed 12 Nov. 2018].

United Nations General Assembly, (1948). *Universal Declaration of Human Rights*. [online] Available at: http://www.un.org/en/universal-declaration-human-rights/ [Accessed 19 Nov. 2018].

Vander Wier, M. (2017). *Are embedded microchips the future? | Canadian HR Reporter*. [online] Canadian HR Reporter. Available at: https://www.hrreporter.com/hr-technology/34390-are-embedded-microchips-the-future/ [Accessed 19 Nov. 2018].

Westby, T. (2018). [online] Linkedin. Available at: https://www.linkedin.com/in/todd-westby-81143843 [Accessed 9 Dec. 2018].

24 Greencoat Place, London SW1P 1BE
t +44 (0) 20 7798 6040 • e info@ibe.org.uk • www.ibe.org.uk

Registered Company No. 11594672
Registered Charity No. 1180741