IBM Analytics
Thought Leadership Whitepaper

IBM® **Smarter Workforce Institute**

My data or your data?

The Evolving Nature of Workers' Privacy Preferences

By Nigel Guenole, Ph.D. and Sheri Feinzig, Ph.D.,
IBM Smarter Workforce Institute

IBM

Employee privacy preferences

Did you know you have control over your privacy settings in applications such as Facebook and LinkedIn? If your answer to this question is "Of course, I wouldn't use them without setting my own preferences" then you might be considered what Westin[1], a pioneer in privacy research, called a Privacy Pragmatist. Those who respond "I will never use those applications because I don't trust what they will do with my information" would be what Westin considered Privacy Fundamentalists. And those whose response is "Really? They have privacy settings?" could be categorized as Privacy Unconcerned.

People's views on data privacy vary widely, not only in the degree of concern, but also in the types of concerns they have. Understanding these views is important because organizations need to obtain personal information from workers to function effectively. However, just how willing workers are to share personal information is unclear. It is also a timely question given recent high profile data privacy breaches that have been described in the news media.

We explored how willing workers are to share different types of information by surveying over 7,000 US workers on their privacy views. In addition to assessing overall levels of privacy sensitivity, we considered concerns specific to the different stages in the management of employee information (collection, storage, usage, and release).

Key findings

Our findings reveal that data privacy attitudes in the US working population have shifted, and become more refined since Westin's original research. We suggest that the grouping of workers according to Westin's original taxonomy of privacy preferences requires some modification. Specific findings include:

- Westin's Pragmatist group is still observable and is the largest group at nearly three quarters of employees.
- The fundamentalist group is also still clearly observable comprising nearly one fifth of employees.
- The final group of nearly one tenth of employees is not unconcerned with privacy as Westin originally defined. In fact, this group showed low concern about data usage and collection, but peaked concern about data storage and release.

As a result of these findings, we recommend organizations develop privacy policies and communication strategies that target each of these revised privacy demographics. The strategies include bringing employee populations into the Pragmatist category, educating Unconcerned employees who need to be more concerned, and assuaging the concerns of Privacy Fundamentalists.

Privacy is a pressing concern for employers and employees

Privacy is the ability to regulate how much information about one's self is known to others[1]. While privacy is acknowledged as critical to successful societal functioning, around the world the tolerance of individuals to having personal information more widely known is being rigorously tested. For example, medical insurers and government departments in the United States have been affected by large-scale privacy breaches in recent years.

Along with the apparent increase in unintentional disclosures of personal information, we are more often asked to intentionally share personal information, both inside and outside the work environment.

However, requests of employees to provide personal information from within the work environment could potentially cause more friction than requests from outside because of different relationship dynamics, such as if a power imbalance exists between employers and employees. For example, a 'request' from a more powerful person such as a manager or boss might be interpreted as a demand by an employee. Even if employees prefer not to share information, they could feel compelled to do so if their livelihoods depend on their work.

Organizations need to manage privacy to function effectively

From an organization's perspective, on the other hand, the ease with which information can be elicited from employees can impact how effectively firms operate. For starters, employees need to relinquish privacy, at least to some degree, so that the day-to-day responsibilities of organizations can be met.

One example many workers have experienced is being asked to trust that personal information in electronic human resource management systems is handled appropriately. In other words, giving up some personal privacy at work allows necessary but prosaic administrative tasks to be undertaken.

More generally, we are seeing a trend where Human Resources is beginning to track what Marketing functions in retail organizations have done for many years. That is to say, moving from treating all employees as though they were the same to customizing its approach and treating employees as segments of one worker.

If HR knows the personal situation and views of the organization's employees, it can begin to tailor policies to suit particular groups of people, and even particular individuals.

This requires a lot more information about the work related thoughts, and feelings, and behaviors of workers (for example, from the analysis of unstructured data such as text in social media posts). But first understanding the employee perspective on sharing this information is critical because HR data are often more sensitive than in marketing settings where it can be easier to 'opt-out'. HR needs to address privacy preferences in a considered way, rather than assuming everyone has the same perspective.

The big question HR needs answered is how resistant are workers to sharing information, and what exactly is it about sharing that they are resisting?

Despite employer requests for information appearing benign compared to unintentional disclosures, such requests still have the potential to limit workers' abilities to control their personal information. For example:

- Workers may be asked to share personal information so that organizations have data for workforce analytics projects
- Employees would need to provide access to information if computer logon times were to be monitored to identify when a worker starts and finishes work
- Organizations may want to text mine discussions on corporate intranet sites

The final example above highlights a further concern; analysts might want to use employee data collected for one purpose in an entirely different analysis. This is known as secondary usage and may not be appropriate. In fact, secondary usage might raise ethical and possibly legal issues. Analyzing workforce data in these circumstances potentially infringes upon workers' ability to control how much personal information is known to their employer, or in other words, their privacy.

Knowing which employees are privacy sensitive can confer a business advantage

One thing seems certain, if firms are to effectively manage their privacy challenges, they need clear information about the prevalence of concern regarding privacy amongst workers. In *Privacy Preferences in the World's Major Economies*, a recent IBM Smarter Workforce Institute report, countries were compared according to their workers' willingness to share personal information for organizational development purposes. In that study, willingness to share information was considered a continuous dimension ranging from low willingness to high willingness. The survey included six items that measured Westin's (1967) three categories: Fundamentalists, Pragmatists and Unconcerned.

While treating preference for privacy as a continuum is appropriate for some purposes, viewing the privacy continuum as discrete categories might also be beneficial. For example, it would help to understand what proportions of your workforce are highly concerned, relatively concerned and unconcerned about privacy. But, more precisely, it would be useful for employers to know what exactly it is that makes employees sensitive about sharing personal information.

If an organization's HR function knows that segments of its workforce are concerned about different aspects of information privacy, then different courses of action ought to follow. For example, some employees may have a principled objection to the collection of personal data, while others may be concerned about data security. Principled objectors might be more likely to be convinced to share information if they see the mutual benefit to both the employee and to the organization that results from sharing the personal information.

On the other hand, those employees whose primary concern is whether the data are stored securely might be more convinced to share information an organization needs if they believe the technological infrastructure that holds the information uses the latest security technology. Knowing whether a workforce is more concerned about whether information is collected, how it is stored, how it is used or whether it is released can help to create more effective communication practices about workplace information privacy.

A new model of worker privacy preferences

To date, there has been no research, of which we are aware, that categorizes the United States workforce into levels of privacy preferences based on specific types of privacy concerns. To examine this issue, we integrate two conceptual models about privacy, Stone et al.'s[2] model that describes aspects of information privacy people are most sensitive about, and Westin's model of individual differences in privacy preferences that classifies people according to their level of sensitivity about privacy.

"...it would help to understand what proportions of your workforce are highly concerned, relatively concerned and unconcerned about privacy."

Stone's model of information privacy concerns

Stone et al. adopted the framework used by the Privacy Protection Study Commission's[3] report when it made recommendations about privacy for organizations. This report offered recommendations for collecting, storing, using and releasing personal information. Importantly, Stone et al. surveyed people's values (views about how things should be), beliefs (what respondents know) and attitudes (degree of favorability) about these different aspects of privacy. Below we provide the definitions of collection, storage, usage and release from Stone et al. We adopted these definitions in the current research.

Collection of information refers to an employee's views about how information should be gathered; values, beliefs, and attitudes about the extent to which organizations currently gather personal information; and attitudes about their ability to control how much information is collected about them. A sample survey statement about values regarding collection that we incorporated in our survey is 'Organizations should be allowed to collect information about people without their permission'.

Storage of information refers to an employee's values, beliefs and attitudes about how organizations should retain information in electronic formats; beliefs about the extent to which organizations currently store their personal information on intranets and the Internet; and beliefs about their ability to influence how much information organizations store about them. A sample statement of beliefs about information storage that we incorporated in our survey is 'I feel 1 have very little power to keep organizations from storing personal information'.

Usage describes an employee's views on how organizations should use their personal information for workforce analytics; their beliefs about the extent to which organizations already do this; and their views on their ability to control the degree to which this occurs. A sample statement regarding attitudes towards information usage is 'I feel quite harassed by the uses that organizations make of personal information about me'.

Release of information refers to an employee's views about how organizations should release information to interested parties; beliefs about the extent to which this is already occurring in the workplace; and attitudes regarding their ability to control how much this happens to them. A sample statement incorporated in our survey regarding values about information release is 'Organizations that collect and store personal information should not have the right to release this information to other organizations'.

Westin's model of individual differences in levels of privacy preferences

Westin argued that privacy describes "the claim of an individual to determine what information about himself or herself should be known to others" and that it plays out at individual as well as organizational and socio-cultural levels. Westin suggested individuals could be categorized by whether they had a low, medium or high preference for privacy, describing people at these different levels as fundamentalists, pragmatists, and those unconcerned with privacy. It is these individual differences that are the primary focus of the current research. Here we present Westin's definitions of these groups of people.

Fundamentalists:

- Distrust organizations that ask for personal information
- Worry about information accuracy and how information is used
- Favor new laws and regulations that specify privacy rights and enforceable remedies

Pragmatists

- Weigh the benefits of consumer opportunities, public safety and personal morality against the intrusiveness of accessing personal information and the increase in government power

Unconcerned

- Generally trustful of organizations collecting personal information
- Comfortable with existing organizational procedures
- Ready to forego privacy claims to secure consumer service benefits or public order values
- Not in favor of the enactment of new privacy laws and regulation

Analysis

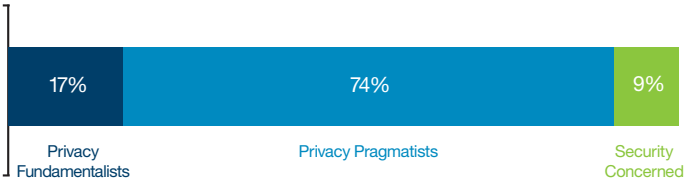
Analysis goals. Our goal was to classify workers using a model that integrates levels of privacy concern from Westin with types of privacy concern from Stone et al. Ratings to survey statements using a five point disagree to agree scale were analyzed with Latent Profile Analysis, a technique for clustering survey respondents into different groups that is preferred today by methodologists looking to uncover unobserved sub-groups in survey responses. We used the technique to attempt to group the responses of over 7,000 US workers to questions about Stone et al.'s types of privacy concern into three different categories of privacy perspectives: Privacy Fundamentalists, Privacy Pragmatists and Privacy Unconcerned, corresponding to the high, medium and low sensitivity to privacy concerns summarized by Westin[1].

Survey questions and sample. The questionnaire used in this study was comprised of twelve statements, of which three statements measured the employee privacy position with respect to data collection, data storage, data usage and data release respectively. The respondents, part of the IBM WorkTrends™ online panel survey, were US employees, from thousands of different companies, who were working 20 hours or more per week, for organizations with over 100 employees, in a range of different industries.

Research results: Is anyone privacy unconcerned anymore?

The first point to note is the size of the three clusters. By far the largest proportion of employees falls into the middle level of concern category, or the class with the second highest average concern for privacy. Figure 1 shows 74 percent of participants can be classified as pragmatists. The next largest class of respondents was fundamentalists, which comprised 17 percent of the overall sample. Finally, 9 percent of employees were classified into the class with the lowest overall concern – although, as we will see they could not be considered entirely unconcerned.

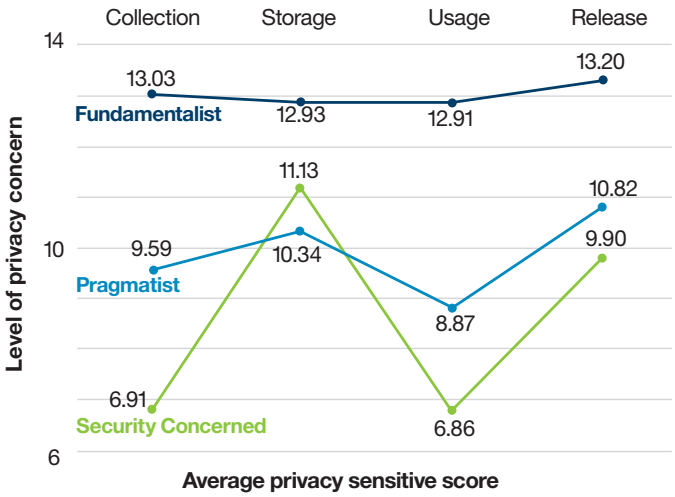
Figure 1. Privacy pragmatists dominate worker population



Source: IBM Kenexa WorkTrends™ 2015 US (Privacy Fundamentalists N= 1,246, Privacy Pragmatists N=5,471, Security Concerned N=688)

When we look at the detail of employee attitudes, values and beliefs within the three groups some interesting differences emerge (see Figure 2). The lowest scoring group overall (green line), rather than being completely unaware or unconcerned, has a different pattern of scores across the four types of concern. The lowest scoring group is indeed less concerned with the initial collection of data and usage of data, but shows a heightened concern with the way the data are stored and whether the data are released.

Figure 2. The privacy concerns of workers vary



Source: WorkTrends™ 2015 US (Privacy Fundamentalists N= 1,246, Privacy Pragmatists N=5,471, Privacy Unconcerned N=688). Each item was scored 1 to 5 on a Likert agreement scale (from 1 strongly disagree to 5 strongly agree). Each 'group' had four items to measure the concepts of collection, storage, usage, and release. The minimum possible score on the x-axis is 4 (4*1) and the maximum possible score is 20 (4*5).

On the other hand, the middle scoring class shows moderate concern across all four types of information privacy concern. Therefore, we suggest a reinterpretation of Westin's three classes for this particular data set. The highest scoring class remains a Privacy Fundamentalist group. However, the lower scoring two classes can both be considered Privacy Pragmatists, with one group showing moderate levels of concern across all areas of the model matching Westin's Privacy Pragmatist definition. The anticipated Privacy Unconcerned group does in fact have two concerns: how the data are stored and whether they are released.

In summary, this research would suggest the following new groupings to categorize employee privacy preferences (revised from Westin's original model):

- Privacy Fundamentalists
- Privacy Pragmatists
- Security Concerned

Conclusions

Our survey of US employees sought to examine whether Westin's three groups of privacy concern could be uncovered amongst the US working population, while at the same time answer the following questions about these groups:

- Is it the collection of the data itself that most concerns people?
- Is it the fact that data are being stored?
- Is it the uses employees believe will be made of the data?
- Or is it the risk of release of personal data by an employer to other parties?

Our results showed that there are three classes representing different levels of concern with privacy that can indeed be recovered from the survey responses. However, these classes are not entirely consistent with the classes originally identified by Westin. While a Fundamentalist class and a Pragmatist class can be identified that show broad alignment with the classes identified by Westin, the Unconcerned class has been replaced by a class with primary concerns about how well data are stored and whether or not they have control over whether and how data are released.

Implications

Our results suggest an evolution toward increased privacy awareness, as well as more nuanced views of privacy held by our survey respondents, potentially a result of publicity around high-profile data breaches. This has the following implications for practitioners:

- **Privacy concerns cannot be ignored**
  No identifiable segment of employees are totally unconcerned with privacy, so organizations today need to ensure they employ effective communication strategies about privacy to all employees.
- **Know your employees' privacy concerns**
  In the same way as this study has assessed privacy concerns of workers in the US, organizations could use survey or polling techniques to assess their own workers' privacy views. This would ensure the most appropriate messaging in communications.
- **Customize communications**
  Once an organization has a clear understanding of its employees' privacy preferences, it can target privacy policies and communications to effectively address the different levels and types of concerns. This research shows that a one-size-fits-all approach will no longer suffice, given the different levels of concern with different dimensions of privacy (i.e., collection, storage, usage and release). It should also be recognized that future changes in the privacy sensitivity of working populations cannot be ruled out, so communications will need to be adapted as employees' views shift.

If you'd like to learn more about IBM's workforce analytics solutions, click here.

IBM Smarter Workforce Institute

The IBM Smarter Workforce Institute produces rigorous, global, innovative research spanning a wide range of workforce topics. The Institute's team of experienced researchers applies depth and breadth of content and analytical expertise to generate reports, white papers and insights that advance the collective understanding of work and organizations. This white paper is part of IBM's on-going commitment to provide highly credible, leading-edge research findings that help organizations realize value through their people.

To learn more about IBM Smarter Workforce Institute, please contact us at ibmswi@us.ibm.com.

Follow @IBMSmtWorkforce on Twitter or visit our website: http://www-01.ibm.com/software/smarterworkforce/institute/

About the Authors

Nigel Guenole, Ph.D.

Nigel Guenole is an Executive Consultant with the Smarter Workforce Institute and a Senior Lecturer in Management at Goldsmiths, University of London. He is known for his work in workforce analytics, statistical modeling and psychological measurement.

Dr. Guenole's work has appeared in leading scientific journals including Industrial Organizational Psychology: Perspectives on Science and Practice and Frontiers in Quantitative Psychology & Measurement, as well as in the popular press. Dr. Guenole is the current external examiner for organizational behavior programs at London School of Economics (LSE) and University College London (UCL). He is a Chartered Occupational Psychologist and an Associate Fellow of the British Psychological Society (BPS). He is registered with the Health & Care Professions Council (HCPC) in the United Kingdom, is a member of the Academy of Management (AoM), and is an international affiliate of the Society for Industrial and Organizational Psychology in the United States (SIOP). At Goldsmiths Dr. Guenole teaches courses on leadership and statistical modelling.

Sheri Feinzig, Ph.D.

Sheri Feinzig is the Director of IBM's Smarter Workforce Institute, and has over 20 years' experience in human resources research, organizational change management and business transformation. Sheri has applied her analytical and methodological expertise to many research-based projects on topics such as employee retention, employee engagement, job design and organizational culture. She has also led several global, multi-year sales transformation initiatives designed to optimize seller territories and quota allocation. Additional areas of expertise include social network analysis, performance feedback and knowledge management. Sheri received her Ph.D. in Industrial/Organizational Psychology from the University at Albany, State University of New York. She has presented on numerous occasions at national conferences and has co-authored a number of manuscripts, publications and technical reports. She has served as an adjunct professor in the Psychology departments of Rensselaer Polytechnic Institute in Troy, New York and the Illinois Institute of Technology in Chicago, Illinois, where she taught doctoral, masters and undergraduate courses on performance appraisal, tests and measures.

References

[1]Westin, A. F. (1967). Privacy and Freedom. New York: Atheneum.

[2]Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology, 68, 459-468.

[3]Privacy Protection Study Commission (1977). Personal privacy in an information society, Washington, D.C., US. Government Printing Office.

IBM Corporation

Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
April 2016

Please Recycle

LOW14329USEN-00